DOMAIN NAME SYSTEM

SECURITY CHECKLIST

Version 2, Release 2

14 April 2006

DISA
FIELD SECURITY OPERATIONS

TABLE OF CONTENTS

Page

SUMMARY OF CHANGES

14 April 2006 Version 2 Release 2

Updated IAVMs
Updated acceptable BIND version levels.
Added VMS 6.0 information and procedures.
Added Vulnerability Key to each PDI for reference.

1. INTRODUCTION

This document contains procedures that enable qualified personnel to conduct a Domain Name System (DNS) Security Readiness Review (SRR). The DNS SRR assesses an organization’s compliance with the Defense Information Systems Agency (DISA) DNS Security Technical Implementation Guidance (STIG). DISA Field Security Operations (FSO) conducts SRRs to provide DISA, Joint Commands, and other Department of Defense (DOD) organizations with a level of confidence that their DNS is secure and can adequately support their mission.

1.1 The Scope of a Review

The primary objects of a DNS SRR are the site’s administrative practices, name servers, and the zones these name servers support. As security is only as strong as the weakest link, the review should cover all of supporting name servers. In some cases, this may not be feasible (e.g., the name server is at a remote site), but if any server supporting a zone is not assessed, this should be clearly documented in the SRR final report.

Organizations may also have several caching name servers – i.e., ones that can resolve client queries, but which are not necessarily authoritative for any DNS records. These are the servers that are listed in the DNS configuration of the computers on the internal network. A DNS SRR should also evaluate all of the organization’s caching name servers, but a sample may suffice if there are resource or time constraints.

Client DNS configuration is outside the scope of the review, which focuses on DNS servers and related administrative, technical and physical controls.

1.2 Recording DNS SRR Results

This document contains survey instruments that can assist a reviewer when collecting data on the organization’s DNS infrastructure. Once information is gathered and evaluated, the reviewer will record findings of Vulnerabilities in the SRR Results Report included later in this document.

Results are also entered into the Vulnerability Management System (VMS). The VMS database stores DNS SRR results by name server and operating system asset. The DNS Checklist is divided into several modules. The Site Administration and Zone Architecture are considered network assets. The Name Server Requirements, BIND Name Server Configuration, UNIX OS Configuration to Support BIND, Windows OS Configuration to Support BIND, Windows 2000 DNS Name Server Configuration, and Cisco CSS Configuration are considered server assets.

1.3 Severity Codes

Each Vulnerability has an associated severity code. The severity codes range between IV and I and are defined as follows:

- Category I findings are any vulnerabilities that provide an attacker immediate access into a machine, gain superuser access, or bypass a firewall.

- Category II findings are any vulnerabilities that provide information that has a high potential of giving access to an intruder.

- Category III findings are any vulnerabilities that provide information that potentially could lead to compromise.

- Category IV vulnerabilities, when resolved, will prevent the possibility of degraded security.

2. SRR REPORT

UNCLASSIFIED UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

The SRR Report documents the findings of the review and also includes basic information about the site and key personnel. Each finding has a corresponding PDI/VUL number. Refer to *Section 3* for detailed procedures on how to complete the report.

2.1 Reviewer Information

Reviewer Information:
Name: ____________________
E-mail Address: ____________________
SIPRNet E-mail: ____________________
Phone # (Commercial): (   ) __________ DSN: __________

2.2 Checklist Information

DNS Checklist Information:
STIG Version: ____________________
Checklist Version ____________________
Date of Review: ____________________
Date of Report: ____________________

2.3 Site/Organization Information

Organization Information:
Name ____________________
Address ____________________
City, State, Zip ____________________

Pre-Trip Preliminary Site POC Information:
Name: ____________________
E-mail Address: ____________________
SIPRNet E-mail: ____________________
Phone # (Commercial): (   ) __________ DSN: __________

IAO Information:
Name: ____________________
E-mail Address: ____________________
SIPRNet E-mail: ____________________
Phone # (Commercial): (   ) __________ DSN: __________

NSO Information:
Name: ____________________
E-mail Address: ____________________
SIPRNet E-mail: ____________________
Phone # (Commercial): (   ) __________ DSN: __________

Network Specialist Information:
Name: ______________________________
E-mail Address: ______________________________
SIPRNet E-mail: ______________________________
Phone # (Commercial): (   ) ____________ DSN: ______________

DNS Database Administrator Information:
Name: ______________________________
E-mail Address: ______________________________
SIPRNet E-mail: ______________________________
Phone # (Commercial): (   ) ____________ DSN: ______________

DNS Software Administrator Information:
Name: ______________________________
E-mail Address: ______________________________
SIPRNet E-mail: ______________________________
Phone # (Commercial): (   ) ____________ DSN: ______________

UNIX System Administrator Information (if applicable):
Name: ______________________________
E-mail Address: ______________________________
SIPRNet E-mail: ______________________________
Phone # (Commercial): (   ) ____________ DSN: ______________

Windows System Administrator Information (if applicable):
Name: ______________________________
E-mail Address: ______________________________
SIPRNet E-mail: ______________________________
Phone # (Commercial): (   ) ____________ DSN: ______________

Cisco CSS DNS Administrator Information (if applicable):
Name: ______________________________
E-mail Address: ______________________________
SIPRNet E-mail: ______________________________
Phone # (Commercial): (   ) ____________ DSN: ______________

2.4 Zone(s) Overview

Zone(s)	Network (e.g., 150.150.4.0)

2.5 Name Server(s) Overview

List all of the organization’s name servers, regardless of whether it was reviewed or not. If it was reviewed, place a “Y” in the “Reviewed?” column. Otherwise, enter an “N.” Note whether the server is a zone master or a resolving server using similar notations in the relevant columns.

Host Name	IP Address / Mask	Zones Supported	Reviewed?	Master Name Server?	Caching Name Server?	Physical Location	OS	DNS Software

This page is intentionally left blank.

3. DNS CHECKLIST INSTRUCTIONS

A single reviewer may perform all of the vulnerability checks or they may be divided among several reviewers, or some vulnerabilities may not apply to the review. The approach on how to distribute the vulnerabilities may depend on several factors, including the environment at the site under evaluation, the size of the review team, and the technical expertise and focus of particular reviewers.

The DNS SRR should begin with the DNS SRR team lead or reviewer contacting the site to be reviewed prior to the onsite review. During this initial contact, information required for a concise and timely SRR should be gathered as completely as possible. *Section 4.1, The Pre-Trip Preliminary Interview*, contains questions to be answered and a listing of required documentation to be provided by the site to be reviewed.

The DNS Checklist is divided to allow the reviewer to select only the vulnerabilities that apply to the reviewed site's environment. There are numerous types of DNS software and operating systems (OSs) that can support the DNS architecture. The DNS Checklist has been divided into several sections to allow the reviewer to select the section(s) which best reflects the DNS architecture of the site being reviewed. There are three levels:

- Site-wide (the Site Administration section)
- Zone-wide (the Zone Architecture section)
- Name server (a combination of the Name Server Security Requirements section and the specific implementation of DNS under review – e.g., BIND, Windows 2000, or CSS DNS)

The sections are broken down into different focus areas to allow for only the checks applicable to a reviewed site to be performed, ease of use, eliminate redundancy, and to save time by reducing the amount of checks the reviewer has to read through and make decisions upon. The reviewer will have to make decisions as to which section to perform based on the DNS software and the name server platform under review prior to the on site visit. VMS 6.0 will aid in the selection as a condition will be applied, along with rules, once the operating system is selected on the asset. If the OS is Windows, the reviewer will not see the Unix vulnerabilities. The sections are grouped into two main groupings; network assets and server assets. The reviewer will always be performing the Site Administration section, Zone Architecture section, and the Name Server Security Requirements section. Once a posture of Local or Root DNS is selected, these vulnerabilities will appear under the asset. VMS 6.0 rules will assist the reviewer in determining the appropriate vulnerabilities of the asset. The following is more of a suggested practice for review.

3.1 Network Asset

3.1.1 Site Administration

This section is to be used at each and every site and the vulnerabilities will appear in VMS 6.0 for all DNS assets. This section encompasses the processes and procedures developed at the site to ensure required site-wide administrative security practices are adhered to. This section is independent of any particular DNS software, platform, or architecture in which DNS is configured. This section addresses security requirements related to site-wide administrative practices and is located in *Section 5, Site Administration section,* of this document.

3.1.2 Zone Architecture

This section is to be used for each and every zone supported at the reviewed site and is applicable for all zones being reviewed, except the root zone on caching servers. The number of times this section is used depends on the number of zones supported. This section is independent of any particular DNS software, platform, or architecture in which DNS is configured. This section addresses security requirements related to zone implementations and is located in *Section 6, Zone Architecture section,* of this document.

3.2 Server Asset

3.2.1 Name Server Security Requirements

This section is to be used for each name server located at the reviewed site and is applicable for all name servers. This section will encompass master name servers as well as caching name servers. The DNS name server platform or software is not to be considered. This section is independent of any particular DNS software, platform, or architecture in which DNS is configured. This section addresses security requirements related to all DNS implementations regardless of the product or the operating system on which it runs and is located in *Section 7, Name Server Security Requirements section,* of this document. Cisco CSS DNS is exempt from this section, as many requirements do not apply*, Section 12, Cisco CSS Configuration section,* is customized to focus on this technology.

3.2.2 BIND Name Server Configuration

This section will encompass each BIND instance, regardless of the platform of the name server and is applicable for all BIND instances. This section is in addition to the Name Server Security Requirements section and is to be used for each and every instance of BIND located at the site to be reviewed. This section is independent of any particular DNS architecture or platform on which BIND is configured. This section addresses security requirements related to all BIND implementations regardless of the operating system, which it is running on and is located in *Section 8, BIND Name Server Configuration section,* of this document.

3.2.3 UNIX OS Configuration to Support BIND

This section is to be used for each UNIX name server running BIND located at the site to be reviewed. This section is in addition to the Name Server Security Requirements section and the BIND Name Server Configuration section and is to be used for each and every UNIX OS name server running BIND. This section addresses security requirements related to BIND and the UNIX operating system in which BIND is running on and is located in *Section 9, UNIX OS Configuration to Support BIND section*, of this document. This section will eventually be incorporated into the UNIX section, at which time it will be eliminated.

3.2.4 Windows OS Configuration to Support BIND

This section is to be used for each Windows name server running BIND located at the site to be reviewed. This section is in addition to the Name Server Security Requirements section and the BIND Name Server Configuration section and is to be used for each and every Windows OS name server running BIND. This section addresses security requirements related to BIND and the Windows operating system, which BIND is running on and is located in *Section 10, Windows OS Configuration to Support BIND section*, of this document. This section will eventually be incorporated into the Windows sections, at which time it will be eliminated.

3.2.5 Windows 2000 DNS Name Server Configuration

This section is to be used for each Windows 2000 DNS implementation located at the site to be reviewed. This section is in addition to the Name Server Security Requirements section and is to be used for each and every Windows 2000 DNS name server. This section addresses security requirements related to Windows 2000 DNS and is located in *Section 11, Windows 2000 DNS Name Server Configuration section*, of this document.

3.2.6 Cisco CSS Configuration

This section is to be used for each and every Cisco CSS device. This section addresses security requirements related to Cisco CSS DNS and is located in *Section 12, Cisco CSS Configuration section*, of this document.

3.3 VMS 6.0 Procedures

Due the migration from VMS 5.4 to VMS 6.0, the procedures for assets and visits has changed significantly. The following is a detailed procedure for performing asset registration and visit information for VMS 6.0 reviews.

AS01 Report

The AS01 report can assist the review by quickly identifying the assets at the location the review is being performed. In the section “Looking at DNS Assets” is a quick step by step instruction in creating the report.

1. **<u>Look at DNS Assets</u>**

a. *Steps*
   i. Reports
   ii. AS01
   iii. Select Computing (SUBMIT)
   iv. Select by Location (SUBMIT)
   v. Select the location
      1. May want to do other reports if your site manages or owns assets that are not located at their site. Check Child Locations if applicable.
   vi. Expand Computing. - Expand Network – Expand Data Network
      1. Check the DNS box
   vii. Submit for DNS Asset Report
   viii. View the following website for further details: https://vmscbt.disa.mil/index.htm

b. *Problems*
   i. The element tree always starts at the top of a page. The element tree only prints for one page. If more data, it is truncated.

VL03 Report

The VL03 report can assist the review by quickly identifying the IAVMs that will be identified to the asset when you select the operating system of the asset. This can be accomplished by performing the following steps.

2. <u>Look at IAVMs assigned to an Operating System</u>

a. *Steps*
   i. Reports
   ii. VL03
   iii. Select Operating System/Application under “Choose a Selection Method”
   iv. Select the appropriate Operating System
   v. Select Generate Report
   vi. May want to do other reports if your site manages or owns assets that are not located at their site. Check Child Locations if applicable.
   vii. View the following website for further details:
   https://vmscbt.disa.mil/index.htm

Performing the Review

If the asset is registered and under the correct location, skip to section titled First Review of the Asset. Ensure that the asset is registered in VMS under the correct organization. The asset must have at least an operating system and an IP or MAC address and a fully qualified domain name (FQDN).

1. <u>Creating/Registering the Asset</u>

When CREATING A NEW asset it is recommended to run a VL03 report to identify the IAVMs that will be assigned to the new asset being created.

a. *Steps*

   i. Expand Asset Findings Maint
   ii. Expand Assets/Findings
   iii. Expand Visits to display the sub-folders. *(Reviewer Only) SA will expand Location and proceed to step vi.*
   iv. Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.
   v. Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.
   vi. Click the yellow folder icon located at the right of ‘Computing’.
   vii. Click the General tab
      - Enter the Host name
      - Note: Use “Managed By” for remote locations being managed.
      - Note: Use “Owner Field” to register asset to parent or child location.
      - Note: Mac level, Confidentiality, & Use are defaulted. Change as required.
   viii. Click the ‘Asset Identification’ tab to enter:
      - I.P. Address or MAC Address: (Must click the “add” button to make it add the IP or MAC)
      - Assign a Fully Qualified Domain Name (FQDN)
   ix. Click the ‘Asset Posture’ tab to add postures to the asset:
      - Expand Network
      - Expand Data Network
      - Expand DNS
      - Mark the check box corresponding to the correct DNS server type: Local DNS or DOD Root (only to be applied for DOD backbone DNS servers)
      - Click ‘>>’ to move all selected options to the ‘Selected’ window
      - Expand the Operating System posture and drill down to the appropriate OS
      - Click ‘>>’ to move all selected options to the ‘Selected’ window
      - Click on System/Enclave - Determine the enclave that the asset is part of. Enter the enclave on the Systems/Enclaves tab of the asset creation / or update screen. For registered enclaves, choose the enclave. If the enclave is not present, ensure that the IAM or Team Lead works with the appropriate site personnel to request an enclave.
      - Click ‘Save’

View the following website for further details:
https://vmscbt.disa.mil/index.htm

2. First Review of the Asset

If the asset is registered and it is the first time it has been reviewed, the following may need to be accomplished.

a. Steps

i. Expand Asset Findings Maint

ii. Expand Assets/Findings

iii. Expand Visits to display the sub-folders. *(Reviewer Only) SA will expand Location and proceed to step vi.*

iv. Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.

v. Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.

vi. Expand 'Computing'.

vii. Expand 'Must Review' *(Reviewer Only) SA will not see 'Must Review', but will proceed to step viii.*

viii. Click Asset name.
   - Verify data in General tab and Asset Identification. For details see Section 1 'Creating the Asset".

ix. Click the 'Asset Posture' tab to add functions to the asset:
   - Expand 'Computing' in the 'Available' window
   - Expand 'Network' in the 'Available' window
   - Expand 'Data Network' in the 'Available' window
   - Expand the asset in the 'Selected' window
   - You should see the selected posture of either Local or Root DNS and an Operating System. Verify the posture is correct. Note: All Assets migrated from VMS 5.4 were tied to an operating system function, however it will be required to add other asset posture functions.
   - Click '>>' to move all selected options to the 'Selected' window
   - Click on System/Enclave - Determine the enclave that the asset is part of. Enter the enclave on the Systems/Enclaves tab of the asset creation / or update screen. For registered enclaves, choose the enclave. If the enclave is not present, ensure that the IAM or Team Lead works with the appropriate site personnel to request an enclave.
   - Click 'Save'

x. Continue with the following section 'Procedures for Review of the Asset' - Must Review'

View the following website for further details:
https://vmscbt.disa.mil/index.htm

3. Procedures for Review of the Asset

If all registration tasks have been accomplished, use the following procedures:

a. *Steps*

   i. Expand Asset Findings Maint
   ii. Expand Assets/Findings
   iii. Expand Visits to display the sub-folders. *(Reviewer Only) SA will expand Location and proceed to step vi.*
   iv. Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.
   v. Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.
   vi. Expand 'Computing'.
   vii. Expand 'Must Review' *(Reviewer Only) SA will not see 'Must Review', but will proceed to step viii.*
   viii. Expand Asset to Review - When you drill down into the asset you will find Vulnerabilities assigned to the DNS component and IAVMs and OS vulnerabilities when the OS is expanded.
   ix. Expand the DNS component and the Vulnerability Key.
   x. Update the 'Status' of the vulnerability
   xi. Identify details on all open vulnerabilities
   xii. If applicable: Apply to other assets by using the 'apply to other Findings' pane.
   xiii. System Administrators should expand the OS assigned to the asset and the IAVMs and vulnerabilities. Verify the OS level meets the required release or patch level.

   Note: Descriptions for Icons and Colors can be obtained in the VMS 6.0 WBT. https://vmscbt.disa.mil/index.htm

4. Verify that all necessary assets were reviewed

a. *Steps*

   i. Asset Findings Maint
   ii. Visits
   iii. Expand visit
   iv. Expand location
   v. Expand computing, non-computing, CNDS as applicable.
   vi. Expand 'Must Review'
      1. If checkmarks are gone, the asset has been reviewed or at a minimum has been opened and something has been changed on the asset.
   viii. Reports
      1. VC06 Asset Compliance Report
      2. Can select an asset or an org.
      3. Select "open" status
      4. Can sort on different fields
      5. Display

a. Finding Comments
b. Finding Long Name
   i. Because it's truncated otherwise
c. Finding Details
d. Vulnerability Discussion

6. VC03 Severity Summary Report
   a. Has numbers only
7. VC01
   a. Used for IAVM Compliance

Note: Additional information can be obtained in the VMS 6.0 WBT. https://vmscbt.disa.mil/index.htm

5. **Add Comments**

a. Steps

i. Visit Maint
ii. Expand Organization the visit is set up for.
iii. Expand Visit
iv. Locate the visit you are working on.
v. Click on CCSD or enclave name.
vi. Comments Tab
vii. Save Changes

Note: Additional information can be obtained in the VMS 6.0 WBT. https://vmscbt.disa.mil/index.htm

6. **Compliance Monitoring**

b. Steps

i. Reports
ii. VC06
iii. Can select an asset or an org.
iv. Select "open" status
v. Can sort on different fields
vi. Display
   1. Finding Comments
   2. Finding Long Name
      a. Because it's truncated otherwise
   3. Finding Details
   4. Vulnerability Discussion
vii. VC03
   1. Has numbers only
viii. VC01
   1. Used for IAVM Compliance

Note: Additional information can be obtained in the VMS 6.0 WBT. https://vmscbt.disa.mil/index.htm

This page is intentionally left blank.

4. OBTAIN REQUIRED INFORMATION FOR REVIEW

The SRR team lead or reviewer should obtain as much as he or she can from the below listed personnel prior to continuing on with the checklist, as this obtained information will greatly assist the reviewer in completing the vulnerabilities and reduce the time required to complete the review.

4.1 The Pre-Trip Preliminary Interview

The SRR team lead or reviewer will have to make contact with the site to be reviewed to identify the Point of Contact (POC), who can provide the required Pre-Trip Preliminary DNS information. This POC must be able to answer the questions in *Section 4.1.1, Pre-Trip Preliminary Interview Questions,* and provide the required documentation and procedures listed in *Section 4.1.2, Pre-Trip Preliminary Procedures and Documentation.*

Prior to the onsite visit, the team lead or reviewer must work with the site to obtain the required information to perform the review in a timely, concise, and professional manner. The team lead or reviewer must obtain answers to the questions listed in *Section 4.1.1, Pre-Trip Preliminary Interview Questions*, and gather the procedures and documentation listed in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures*. Obtaining this information prior to the site visit will enable the reviewer to reduce the time the reviewer spends onsite and better prepare the reviewer with knowledge of the site to be reviewed. This will also provide the site with some foreknowledge of the information required for the review and time to gather this information in a more structured manner. The SRR team member should contact the site in a timely manner as to allow the site to be reviewed time to answer the listed questions and to gather and provide the required documentation.

4.1.1 Pre-Trip Preliminary Interview Questions

The SRR team member must make every attempt to obtain answers to these questions prior to the onsite visit. The reviewer must work with the site's POC, who was identified in *Section 4.1, The Pre-Trip Preliminary Interview*, prior to the onsite visit to ensure the below questions are answered as completely as possible.

A. What DNS domains are associated with the organization for which the site has responsibility?

B. How are the domains aggregated into DNS zones?

C. For each zone, what are the host names and physical locations of each of the name servers supporting that zone? Which of these is the master name server for the domain, and which are slaves?

D. What are the host names and physical locations of each of the name servers that resolve DNS queries on behalf of DNS client computers over which the site has responsibility? (These could possibly be the same name servers specified in the answer to question C.)

E. Who is an appropriate person who can provide DNS SRR personnel with information related to the network infrastructure, including IP network, router and firewall configuration. This might be the Network Security Officer, DNS Administrator, or another individual with a good working knowledge of the local environment. What is the phone number and e-mail address of this individual?

F. Who is an appropriate person to provide DNS SRR personnel with a facility tour in which the personnel can see the name servers, supporting network infrastructure, and associated physical and environmental controls. What is the phone number and e-mail address of this individual?

G. For each name server undergoing evaluation, what software currently provides DNS server functionality (e.g., BIND, CSS, and/or Windows 2000 DNS)? What version of the software is installed (e.g., BIND 9.2.1)?

The worksheets in *Appendix A.1, The Pre-Trip Preliminary Interview Survey Instrument*, can assist the reviewer with the collection of this information.

4.1.2 Pre-Trip Preliminary Documentation and Procedures

The SRR team member reviewer must make every attempt to obtain the required documentation and procedures prior to the onsite visit. The reviewer must work with the site's POC, which was identified in *Section 4.1, The Pre-Trip Preliminary Interview*, prior to the onsite visit to ensure the below listed documentation and procedures are gathered as completely as possible.

The SRR team member will obtain copies of all listed documentation and procedures for examination. The reviewer may receive these files from the site's POC in any one of the following forms, listed in order of preference:

- CD-ROM
- Diskette
- Signed, encrypted e-mail
- Paper printout

The reviewer should validate the obtained DNS configuration and zone files – either by witnessing the SA copy and/or print the files or by comparing the files provided with the corresponding ones on the name server itself.

Listed below are the required procedures and documentation to be obtained:

- Procedures

  - DNS operating procedures, to include:
    - Configuration data backup procedures
    - Resource (zone) data backup procedures
  - Procedures for reviewing DNS logs
  - Procedures for manually updating zone records, to include:
    - The process for updating zone records
    - Who is authorized to submit and approve update requests
    - How the DNS database administrator verifies the identity of the person from whom he or she received the request
    - How the DNS database administrator documents any changes made
  - TSIG key supersession procedures, to include:
    - Frequency of key supersession
    - Criteria for triggering emergency supersession events
    - Notification of relevant personnel during emergency and non-emergency supersession
    - Methods for securely transferring newly generated keys

- Documentation

  - DNS configuration change log
  - Log of date and time of patch installs and DNS software upgrades
  - Copy of the DNS configuration files
  - Copy of the zone files
  - List of personnel authorized to administer each zone and name server. This is to include the primary and backup DNS (database and software) administrators for each zone and name server and any SA having root or administrative privileges, to include:
    - Name
    - Phone number
    - E-mail address
  - DNS configuration change log, to include:
    - Date and time any DNS configuration files were modified
    - Business justification for that modification
  - DNS zone record documentation, to include:
    - Owner of each zone record
    - Date the zone record was created
    - Date the zone record was last modified
    - Date the zone record was last verified
  - Network diagrams (both physical and network-layer representations)
  - IP address ranges for:
    - DMZ or perimeter networks
    - Internal networks

All attempts should be made to obtain the required procedures and documentation prior to arrival at the site to be reviewed. In some cases, documentation may be more difficult to obtain, such as the network diagrams and the DNS configuration and zone files. This may be based on the site's desire or ability to release this information prior to the onsite visit.

4.2 The Network Specialist Interview

During the pre-trip preliminary interview, *Section 4.1.1*, *Pre-Trip Preliminary Interview Questions*, Question E, the reviewer will learn who is the most appropriate person to direct questions regarding the network infrastructure. The reviewer will schedule an interview with the network specialist do obtain background information on the network. Much of this information will assist the reviewer in determining compliance with later checklist items. For example, information collected on local IP networks and subnets will be utilized during both the review of the configuration and zone files. Some findings, however, can be based on the results of this interview alone. The objective is to obtain all network related information in one session to avoid repeated interruptions during the course of the review.

4.2.1 Network Specialist Interview Questions

The reviewer may use his or her judgment to determine the best way to conduct the interview, but must obtain the answers to the following questions:

A. What IP networks and subnets comprise the internal network?

B. What IP subnets comprise the organization's DMZ(s)?

C. What is the physical location (building or site) of each of the networks or subnets specified in the responses to Question A and B?

D. What is the IP address and subnet mask of each of the name servers listed in response to Pre-Trip Preliminary Interview Question C?

E. Where are firewall devices located within the network infrastructure? What are the IP addresses of each of the firewall interfaces?

F. How do firewall rules and router ACLs restrict access to the listed name servers? Which of the name servers are accessible from external hosts?

G. If Network Address Translation (NAT) is used for particular hosts in a DMZ or on an internal network, then what the actual and translated IP addresses for those hosts?

H. Does anyone in the organization administer a name server from a computer residing outside of the enclave? If yes, where are the clients located and which name servers are administered in this manner? What software, if any, is used to encrypt network traffic between client and server?

The worksheets in *Appendix A.2, The Network Specialist Interview Survey Instrument,* can assist the reviewer with the collection of this information.

4.3 The DNS Administrator Interview

During the pre-trip preliminary interview, *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures,* the reviewer obtained the names of the authorized DNS administrators for each zone. The reviewer should interview at least one listed DNS administrator for each zone. One individual, however, can answer for many zones so long as that individual is an authorized DNS administrator for each of those zones. The objective is to obtain all DNS configuration related information in one session to avoid repeated interruptions during the course of the review.

4.3.1 DNS Administrator Interview Questions

The reviewer may use his or her judgment to determine the best way to conduct the interview, but must obtain the answers to the following questions:

A. How are DNS logs archived (i.e., to what storage medium using what process?) How long are the archived files stored before deletion or destruction?

B. How are operating system logs archived (i.e., to what storage medium using what processes)? How long are the archived files stored before deletion or destruction?

The worksheets in *Appendix A.3, The DNS Administrator Interview Survey Instrument,* can assist the reviewer with the collection of this information.

4.4 The CSS Administrator

During the pre-trip preliminary interview, *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures,* the reviewer obtained the names of the authorized DNS administrators for each zone. Different sites may use different personnel strategies to manage DNS servers. At some sites, the individual who supports the CSS DNS name server may be different from the person who administers the DNS zones, while at other sites the same person may perform both functions. Due to the nature of the CSS DNS name server, the DNS STIG and Checklist will take for granted the CSS zone data, and configuration is supported by an administrator supporting both roles.

4.4.1 CSS Administrator Interview Questions

A. What is the length of the session_key used when configuring the APP CHAP authentication and MD5? How was the key generated (i.e., randomly created)?

This page is intentionally left blank.

5. SITE ADMINISTRATION

This section is to be used at each and every site and only once per site and is applicable for all sites being reviewed. This section encompasses the processes and procedures developed at the site to ensure required site-wide administrative security practices are adhered to. This section is independent of any particular DNS software, platform, or architecture in which DNS is configured.

The DNS SRR begins by completing the *Section 4.1*, *The Pre-Trip Preliminary Interview*, which includes obtaining answers to questions and gathering written documentation and procedures, and configuration and zone files prior to the onsite visit. In addition to the pre-trip information gathered, completion of *Section 4.3*, *The DNS Administrator Interview,* and *Section 4.4*, *The CSS Interview*, if applicable, is required to accurately complete this section. Additionally, an SA will be required to assist in the console-based checks within this section.

5.1 Vulnerabilities

Complete this entire form for each site being reviewed. For each Vulnerability, check whether it is a “Finding” or “Not a Finding” in the “Status” column. In cases in which the Vulnerability is not applicable, check “Not Applicable” (e.g., it applies to an authoritative server, but you are reviewing a caching server). If a Vulnerability is relevant to the environment, but you are unable to evaluate it for whatever reason (e.g., access restrictions or time limitations), then check “Not Reviewed.”

5.1.1 Checks Associated with Interview Responses

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	Script	Status	Details		PDI/VUL	Description	Cat.
5.2.1		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0100 V0004451	A caching name server is not protected by equivalent or better physical access controls than the clients it supports.	2
5.2.1		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0105 V0004452	An authoritative name server is not protected by equivalent or better physical access controls than each of the hosts in its zone.	2
5.2.2		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0110 V0004453	The DNS log archival requirements do not meet or exceed the log archival requirements of the operating system on which the DNS software resides.	2

5.1.2 Checks Associated with Documentation and Procedures

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	**Script**	**Status**	**Details**		**PDI/VUL**	**Description**	**Cat.**
5.3.1		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0115 V0004454	DNS logs are not reviewed daily or a real-time log analysis or network management tool is not employed to immediately alert an administrator of critical DNS system messages.	2
5.3.2		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0120 V0004455	A list of personnel authorized to administer each zone and name server is not maintained.	4
5.3.3		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0125 V0004456	A zone or name server does not have a backup administrator.	2
5.3.4		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0130 V0004457	A patch and DNS software upgrade log is not maintained.	2
5.3.5		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0135 V0004458	Operating procedures do not require that DNS configuration and resource record data be backed up on each day on which there are changes.	2

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	Script	Status	Details		PDI/VUL	Description	Cat.
5.3.6		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0140 V0004459	Configuration change logs are not maintained.	2
5.3.7		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0145 V0004460	Key supersession procedures are inadequate.	2
5.3.6		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0150 V0004461	Procedures for updating zone files are inadequate.	2

5.2 Checks Associated with Interview Responses

The questions asked in *Section 4.1.1 Pre-Trip Preliminary Interview Questions,* and *Section 4.3.1, DNS Administrator Interview Questions* will enable the reviewer to complete this section.

5.2.1 Physical Access Control

RFC 2870 states that the specific area in which the name server is located must have positive access control. In other words, the number of individuals permitted access to the area must be limited, controlled, and recorded. At a minimum, control measures should include mechanical or electronic locks.

These protection mechanisms are highly recommended, but may not be feasible at all sites. Name servers, however, should be among the most secured computers at a location because compromise of a name server can directly impact the security of the services it supports. For example, a facility should not house web servers in a locked cage within a secured data center, but allow a name server that resolves the IP addresses for those web servers to reside on an administrator's desk.

Instruction: Based on the answer to Question C in *Section 4.1.1, Pre-Trip Preliminary Interview Questions,* ask to see the locations at the facility where computers supported by the listed name server(s) under evaluation are located (e.g., server closets, raised floor space, etc.). Note those areas that have the most extensive physical security controls. Also ask to see the locations of the name servers themselves. Then compare the physical security of the most secure computers against the physical security of the name server under evaluation. If the name server has substantially weaker physical security controls than the hosts it supports (e.g., the name server is in the DNS administrator’s cube while the servers are in a locked cage in a secure raised floor area), then this is a finding.

The reviewer should avoid making minor distinctions between various forms of physical security. The intent of the PDI/VUL is to identify significant violations of the requirement.

PDI:	DNS0100	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		COEB-1, COEB-2, DCCS-1, DCCS-2, DCBP-1	
Vulnerability Description:		A caching name server is not protected by equivalent or better physical access controls than the clients it supports.	
Reference:		DNS STIG: Sec. 7.1.2	

PDI:	DNS0105	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		COEB-1, COEB-2, DCCS-1, DCCS-2, DCBP-1	
Vulnerability Description:		An authoritative name server is not protected by equivalent or better physical access controls than each of the hosts in its zone.	
Reference:		DNS STIG: Sec. 7.1.2	

5.2.2 Archival Requirement

Instruction: This check is only applicable if DNS logs are independent from system logs. If they are, then compare the answers to Question A and B in *Section 4.3.1, DNS Administrator Interview Questions*. If the log archival scheme for the DNS logs is weaker than the one for the system logs, then this is a finding.

PDI:	DNS0110	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		ECAT-1, ECAT-2, DCCS-1, DCCS-2	
Vulnerability Description:		The DNS log archival requirements do not meet or exceed the log archival requirements of the operating system on which the DNS software resides.	
Reference:		DNS STIG: Sec. 7.3.3	

5.3 Checks Associated with Review of Documentation and Procedures

The documentation and procedures, obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures,* will enable the reviewer to complete this section.

Judgments as to whether the procedures are adequate should not be based on the subjective opinion of the reviewer. Rather, the reviewer should limit the review to identifying whether required elements of the procedures exist.

5.3.1 DNS Log Files

Instruction: Review the procedures for reviewing DNS logs, obtained in *Section 4.2.1, Pre-Trip Documentation and Procedures*, if reviewing of logs is anything less than daily, then this is a finding. In many cases, DNS logs are included within the system logs. If this is the case, then daily review of the system logs meets the requirement. If the site employs special software to scan logs for special events or key words, then this is also acceptable so long as the system issues real time alerts or is monitored at least daily.

PDI:	DNS0115	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		VIVM-1, DCCS-1, DCCS-2, ECSC-1	
Vulnerability Description:		DNS logs are not reviewed daily or a real-time log analysis or network management tool is not employed to immediately alert an administrator of critical DNS system messages.	
Reference:		DNS STIG: Sec. 7.3.3	

5.3.2 Personnel Documentation

Instruction: The list of personnel authorized to administer each zone and name server is obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures*. If the site POC cannot produce a list of backup personnel authorized to administer each zone and name server, then this is a finding.

PDI:	DNS0120	Category:	IV
MAC/Confidentiality Levels:	MAC I – CSP, MAC II – CSP, MAC III – CSP		
IA Controls:	PRMP-1, PRMP-2, ECPA-1		
Vulnerability Description:	A list of personnel authorized to administer each zone and name server is not maintained.		
Reference:	DNS STIG: Sec. 7.1.1		

5.3.3 DNS Administrators

Instruction: The list of personnel authorized to administer each zone and name server is obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures*. If the site POC cannot produce a list of backup personnel authorized to administer each zone and name server, then this is a finding. If any zone or name server has only one DNS database administrator or only one DNS software administrator, then this is a finding. If there is not a backup administrator for both roles, then this is a finding.

PDI:	DNS0125	Category:	II
MAC/Confidentiality Levels:	MAC I – CSP, MAC II – CSP, MAC III – CSP		
IA Controls:	DCBP-1		
Vulnerability Description:	A zone or name server does not have a backup administrator.		
Reference:	DNS STIG: Sec. 7.1.1		

5.3.4 Patches and Upgrades

DNS patch and upgrade change records obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures*, must include records of the date and time each patch or upgrade to DNS software was implemented. The method of verification may be considered weak, but the requirement is merely to document the dates and times of DNS software patch and upgrades.

Instruction: If there is no patch and upgrade log, then this is a finding. If there is such a log, then entries must include the date and time of any change. Failure to include this information for any entry is a finding.

PDI:	DNS0130	Category:	II
MAC/Confidentiality Levels:	MAC I – CSP, MAC II – CSP, MAC III – CSP		
IA Controls:	DCBP-1		
Vulnerability Description:	A patch and DNS software upgrade log is not maintained.		

Reference:	DNS STIG: Sec. 7.2.1

5.3.5 Backup

Fortunately, by design, the DNS architecture provides built-in redundancy support. There should always be a hot backup of zone information present whenever the primary name server is unavailable for any reason (i.e., the authoritative slave server maintains a copy of the zone files on the master). This built-in redundancy, however, does not extend to configuration files and logs. Therefore, name servers should be backed up to an external media (e.g., tape, optical disk, etc.) on a regular basis.

At some locations, an automated enterprise backup system supports many servers. In this case, name servers can simply be added to the enterprise system. At other locations, backups must be performed manually, placing a considerably higher burden on administrators. In circumstances in which zone and configuration information is very static, remaining the same for several months at a time, it would make little sense to conduct daily full backups. Backups should occur as frequently as needed to capture changes on the name server.

Instruction: The DNS operating procedures are obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures.* If there are no written procedures for the backup of name servers, then this is a finding. Backup in this context refers to copying the name server's DNS configuration and resource record data, at a minimum, in case it is needed for recovery at a later time. A full file system backup of the name server is preferred.

If there are written backup procedures, then it must call for the backup of DNS configuration and resource record data on any day in which they were modified, it this is not the case, then this is a finding. Any traditional daily tape backup scheme – whether it involves a full, incremental or differential scheme – will satisfy the requirement. Less frequent backups will also suffice if the configuration and resource record data are backed up whenever they are modified.

PDI:	DNS0135	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	DCBP-1		
Vulnerability Description:	Operating procedures do not require that DNS configuration and resource record data be backed up on each day on which there are changes.		
Reference:	DNS STIG: Sec. 7.2.2		

5.3.6 DNS Configuration File Changes

The DNS configuration change log, obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures,* must note the date and time any DNS configuration files were modified and the business justification for that modification. Unless the business justification is routinely so vague as to be meaningless (e.g., "user request" for every entry), the reviewer should not second-guess what constitutes an acceptable business rationale.

Instruction: If there is no configuration change log, then this is a finding. If there are such records, then entries must include the date and time of any change and the business rationale for the change. Failure to include this information for any entry is a finding.

PDI:	DNS0140	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECSD-1, ECSD-2, DCBP-1		
Vulnerability Description:	Configuration change logs are not maintained.		
Reference:	DNS STIG: Sec. 7.3.1		

5.3.7 Cryptographic Key Supersession

Like user account passwords, cryptographic keys such as TSIG keys must be changed periodically to minimize the probability that they will be compromised. If there is a known compromise of a TSIG key, then it needs to be replaced immediately. One of the most important aspects of key supersession is the method that will be used to transfer newly generated keys. Possibilities, in rough order of preference, are as follows:

- SSH
- Encrypted e-mail using DOD PKI certificates (preferred) or PGP
- Secure fax (STU-III)
- Regular mail (using the expedited mailing service holding the current GSA contract for "small package overnight delivery service")
- Hand courier

Instruction: If there are no procedures for TSIG key supersession, obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures*, then this is a finding. If there are such procedures, then it must cover the following:

- Frequency of key supersession
- Criteria for triggering emergency supersession events
- Notification of relevant personnel during emergency and non-emergency supersession
- Methods for securely transferring newly generated keys

This is a finding if any of these elements are missing from the supersession procedures.

PDI:	DNS0145	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	DCBP-1		
Vulnerability Description:	Key supersession procedures are inadequate.		
Reference:	DNS STIG: Sec. 7.3.2		

5.3.8 DNS Database Administration Responsibilities

To best assure the integrity of zone files, one must not only carefully manage the manner in which requests are processed but also periodically check that the current records are valid. For example, when equipment is retired, people often fail to remove the associated host from the DNS. Without periodic checks, an attacker may use a retired host IP address to obtain valuable information from another user who was unaware of the change.

Instruction: If there are no written procedures, obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures,* for manual updates of zone files (e.g., a new host entry), then this is a finding. If there are such procedures, then it must cover the following:

- The process for updating zone records
- Who is authorized to submit and approve update requests
- How the DNS database administrator verifies the identity of the person from whom he or she received the request
- How the DNS database administrator documents any changes made

This is a finding if any of these elements are missing from the procedures for manually updating zone records.

PDI:	DNS0150	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECSD-1, ECSD-2, ECSC-1		
Vulnerability Description:	Procedures for updating zone files are inadequate.		
Reference:	DNS STIG: Sec. 7.4		

6. ZONE ARCHITECTURE

The DNS SRR begins by completing the *Section 4.1, The Pre-Trip Preliminary Interview*, which includes obtaining answers to questions and gathering written documentation and procedures, and configuration and zone files prior to the onsite visit. In addition to the pre-trip information gathered, completion of *Section 4.2, The Network Specialist Interview,* is required to accurately complete this section.

6.1 Vulnerabilities

Complete this entire form for each zone being reviewed. For each Vulnerability, check whether it is a finding or not a finding in the "Status" column. In cases in which the Vulnerability is not applicable, check "Not Applicable" (e.g., it applies to an authoritative server, but you are reviewing a caching server). If a Vulnerability is relevant to the environment, but you are unable to evaluate it for whatever reason (e.g., access restrictions or time limitations), then check "Not Reviewed."

6.1.1 Checks Associated with Interview Response

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	**Script**	**Status**	**Details**		**PDI/VUL**	**Description**	**Cat.**
6.2.1		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0200 V0004462	An authoritative master name server does not have a slave.	1
6.2.2		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0205 V0004463	All of the name servers authoritative for a zone are located on the same network segment.	1

6.1.2 Checks Associated with Review of Documentation and Procedures

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	**Script**	**Status**	**Details**		**PDI/VUL**	**Description**	**Cat.**
6.3.1		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0210 V0004464	Name servers are not geographically distributed.	2
6.3.2		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0215 V0004465	A zone is not supported by a split DNS configuration.	3
6.3.3		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0220 V0004466	Zone records are not adequately documented.	3

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	**Script**	**Status**	**Details**		**PDI/VUL**	**Description**	**Cat.**
6.3.4		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0225 V0004467	A zone record has not been validated in over a year.	2
6.3.5		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0230 V0004468	The zone file contains a host record for a host outside the zone.	3
6.3.6		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0235 V0004469	A CNAME record has been active for more than six months.	4
6.3.7		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0240 V0004470	Zone file contains invalid NS records.	1

6.2 Checks Associated with Interview Responses

The questions asked in *Section 4.1.1 Pre-Trip Preliminary Interview Questions,* and *Section 4.2.1, Network Specialist Interview Questions,* will enable the reviewer to complete this section.

6.2.1 Redundant Name Servers

Instruction: Using the answer to Question C in *Section 4.1.1, Pre-Trip Preliminary Interview Questions,* identify any zone that does not have a slave. An authoritative server for each zone must have a slave name server. If this is not the case, then this is a finding.

PDI:	DNS0200	Category:	I
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	CODB-3, ECSC-1, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	An authoritative master name server does not have a slave.		
Reference:	DNS STIG: Sec. 3.3		

6.2.2 Network Segment

Instruction: Using both the information regarding which servers support each zone from Question C in *Section 4.1.1, Pre-Trip Preliminary Interview Questions,* and the information regarding the IP address and subnet mask of each name servers from question D in *Section 4.2.1, Network Specialist Interview Questions,* determine whether all the name servers supporting the same zone reside on the same subnet. If this is the case, there is a finding.

PDI:	DNS0205	Category:	I
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	CODB-3, ECSC-1, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	All of the name servers authoritative for a zone are located on the same network segment.		
Reference:	DNS STIG: Sec. 3.3		

6.3 Checks Associated with Review of Documentation and Procedures

The documentation and procedures, obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures,* will enable the reviewer to complete this section.

Judgments as to whether the procedures are adequate should not be based on the subjective opinion of the reviewer. Rather, the reviewer should limit the review to identifying whether required elements of the procedures exist.

6.3.1 Hosts Locations

Instruction: Using information from answer to Question C in *Section 4.2.1, Network Specialist Interview Questions,* and an examination of the zone file, obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures*, the reviewer can determine whether there are hosts defined on one of the name server's zones that reside in more than one building. If they all reside in the same building, then this check does not apply. If the defined hosts reside in different buildings, then one of the evaluated name server's zone partners (slave or master) must reside in an alternate building. In this case, if all of the authoritative name servers for a zone reside in the same building, then this a finding.

PDI:	DNS0210	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		CODB-3, ECSC-1, COAS-1, COAS-2, DCCS-1, DCCS-2, DCBP-1	
Vulnerability Description:		Name servers are not geographically distributed.	
Reference:		DNS STIG: Sec. 3.3	

6.3.2 Split DNS

Instruction: If examination of a zone file, obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures*, demonstrates that it includes externally accessible hosts (IP addresses outside of internal address ranges), then the name server must support a split DNS configuration. This should be evidenced by the use of the *view* statement in the *named.conf* file. If it is not, then the DNS administrator must satisfactorily explain how an alternative mechanism achieves the same effect. If externally accessible hosts are supported and a split DNS configuration is not employed or a satisfactory alternative mechanism is not employed, then this is a finding. The objective is that an external DNS client should have no means of querying the DNS to obtain a host-to-IP-address mapping for an internal host.

PDI:	DNS0215	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		ECCD-1, ECSC-1, DCCS-1, DCCS-2, DCBP-1	
Vulnerability Description:		A zone is not supported by a split DNS configuration.	
Reference:		DNS STIG: Sec. 3.4.2.1	

6.3.3 Zone Record Documentation

DNS zone record documentation will preferably reside in the zone file itself through comments, but if this is not feasible, the DNS database administrator will maintain a separate database for this purpose.

Instruction: Review the zone files and the DNS zone record documentation, obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures,* if the records are not fully documented, then this is a finding. The zone record documentation is to include, at a minimum:

- The owner of each zone record
- The date the zone record was created
- The date the zone record was last modified
- The date the zone record was last verified

Records can be grouped (e.g., a number of workstations residing in the same area or a high-availability server cluster)

PDI:	DNS0220	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECSC-1, DCBP-1		
Vulnerability Description:	Zone records are not adequately documented.		
Reference:	DNS STIG: Sec. 3.6.1		

6.3.4 Zone Record Validation

Instruction: When checking the DNS zone record documentation, obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures*, the reviewer should also check that the record’s last verified date is less than one year prior to the date of the review. If this is not the case for any host or group of hosts, then this is a finding.

PDI:	DNS0225	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECSC-1, DCBP-1		
Vulnerability Description:	A zone record has not been validated in over a year.		
Reference:	DNS STIG: Sec. 3.6.1		

6.3.5 Extraneous Resource Records

Instruction: Review the zone files, obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures*, and confirm with the DNS administrator that the hosts defined in the zone files do not reside in another zone with its fully qualified domain name. If extraneous resource records are maintained, then this is a finding.

PDI:	DNS0230	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	DCCS-1, DCCS-2, ECSC-1, DCBP-1		
Vulnerability Description:	The zone file contains a host record for a host outside the zone.		
Reference:	DNS STIG: Sec. 3.6.2		

6.3.6 Zone-spanning

Instruction: Review the zone files and the DNS zone record documentation, obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures,* and confirm that there are no CNAME records older than 6 months. If there are CNAME records older than 6 months, then this is a finding.

PDI:	DNS0235	Category:	IV
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		DCCS-1, DCCS-2, ECSC-1, DCBP-1	
Vulnerability Description:		A CNAME record has been active for more than six months.	
Reference:		DNS STIG: Sec. 3.6.2	

6.3.7 NS Records

Instruction: Review the zone files, obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures,* and confirm with the DNS administrator that each NS record points to an active name server authoritative for the domain, it this is not the case, then this is a finding. The answer to Question C in *Section 4.1.1*, *Pre-Trip Preliminary Interview Questions*, will aid in validating this requirement.

PDI:	DNS0240	Category:	I
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		DCCS-1, DCCS-2, ECSC-1, DCBP-1	
Vulnerability Description:		Zone file contains invalid NS records.	
Reference:		DNS STIG: Sec. 3.6.3	

This page is intentionally left blank.

7. NAME SERVER SECURITY REQUIREMENTS PDL

This section is to be used for each name server located at the reviewed site and is applicable for all name servers. This section will encompass master name servers as well as caching name servers. The DNS name server platform or software is not to be considered. This section is independent of any particular DNS software, platform, or architecture in which DNS is configured. This section addresses security requirements related to all DNS implementations regardless of the product or the operating system on which it runs. Cisco CSS DNS is exempt from this section, as many requirements do not apply*, Section 12, Cisco CSS Configuration section*, is customized to focus on this technology.

At this time, the only DISA approved operating systems and versions of these operating systems to support DNS server software are:

- Sun Solaris 2.6 and above
- HP-UX 10 and above
- Windows NT 4.0
- Windows 2000 and 2003

At this time, the only DISA approved DNS software and versions are:

- BIND 9.2.1
- BIND 9.2.1 for Microsoft Windows NT, Windows 2000, and Windows 2003
- Windows 2000 DNS
- CSS DNS

The currently permitted is Cisco CSS DNS limited to hosts defined in the csd.disa.mil domain.

Guidance for performing checks are documented for the above listed operating systems and DNS software implementations, as these are the DISA approved operating systems. As time progresses additional guidance will be provided if Cisco CSS DNS becomes more commonplace and as additional operating systems and DNS software implementations are added to this list.

The DNS SRR begins by completing the *Section 4.1, The Pre-Trip Preliminary Interview*, which includes obtaining answers to questions and gathering written documentation and procedures, and configuration and zone files prior to the onsite visit. In addition to the pre-trip information gathered, completion of *Section 4.2, The Network Specialist Interview,* and Section *4.3, The DNS Administrator Interview*, is required to accurately complete this section. Additionally, an SA will be required to assist in the console-based checks.

Complete this entire form for each site being reviewed. For each PDI/VUL, check whether it is a “Finding” or “Not a Finding” in the “Status” column. In cases in which the PDI/VUL is not applicable, check “Not Applicable” (e.g., it applies to an authoritative server, but you are reviewing a caching server). If a PDI/VUL is relevant to the environment, but you are unable to evaluate it for whatever reason (e.g., access restrictions or time limitations), then check “Not Reviewed.”

7.1.1 Checks Associated with Interview Response

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	Script	Status	Details		PDI/VUL/	Description	Cat.
7.2.1		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0400 V0004471	The name server software on production name servers is not BIND or Windows 2000 DNS.	2
7.2.2		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0405 V0004472	Hosts outside an enclave can directly query or request a zone transfer from a name server that resides on the internal network (i.e., not in a DMZ).	2

7.1.2 Console-based Checks

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	**Script**	**Status**	**Details**		**PDI/VUL**	**Description**	**Cat.**
7.3.1		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0410 V0004474	DNS server software does not run on an approved operating system.	2
7.3.2		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0415 V0004473	DNS software does not run on dedicated hardware.	2
7.3.3		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0420 V0004475	File permissions on files containing DNS encryption keys are inadequate.	2
7.3.4		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0425 V0004476	File permissions on DNS zone files are inadequate.	2
7.3.5		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0430 V0004477	File permissions on DNS configuration files are inadequate.	2
7.3.6		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0435 V0004478	The name server’s IP address is not statically defined.	2

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	**Script**	**Status**	**Details**		**PDI/VUL**	**Description**	**Cat.**
7.3.7		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0440 V0004479	An integrity checking tool is not monitoring for any modifications to the root hints and name server configuration files.	2
7.3.8		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0445 V0004480	A cryptographic key used to secure DNS transactions has been utilized on a name server for more than one year.	2

7.1.3 Checks Associated with Review of Documentation and Procedures

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	**Script**	**Status**	**Details**		**PDI/VUL**	**Description**	**Cat.**
7.4.1		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0450 V0004481	Dynamic updates are enabled and not cryptographically authenticated.	1
7.4.2		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0455 V0004482	A slave supporting a zone does not cryptographically authenticate its master before accepting zone updates.	1 or 2
7.4.3		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0460 V0004483	A zone master server does not limit zone transfers to a list of active slaves authoritative for that zone.	3
7.4.4		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0465 V0004484	A zone master server does not cryptographically authenticate slaves requesting a zone transfer.	3
7.4.5		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0470 V0004485	A name server is not configured to only accept notifications of zone changes from a host authoritative for that zone.	2
7.4.6		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0475 V0004486	Recursion is not prohibited on an authoritative name server.	3

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	**Script**	**Status**	**Details**		**PDI/VUL**	**Description**	**Cat.**
7.4.7		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0480 V0004487	A caching name server does not restrict recursive queries to only the IP addresses and IP address ranges of known supported clients.	3
7.4.8		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0485 V0004488	Name server logging is inadequate.	1 or 2
7.4.9		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0490 V0004489	Name server logs are not adequately secured.	2
7.4.10		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0495 V0004490	Entries in the name server logs do not contain timestamps and severity information.	3
7.4.11		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0500 V0004491	The local root zone file contains an invalid root name server entry.	1
7.4.12		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0505 V0004492	The root hints file on an authoritative name server is not deleted.	3

7.2 Checks Associated with Interview Responses

The questions asked in *Section 4.1.1, Pre-Trip Preliminary Interview Questions,* and *Section 4.2.1 Network Specialist Interview Questions,* will enable the reviewer to complete this section. Additionally, a Windows SA will be required to assist in the console-based checks within this section if reviewing a Windows 2000 DNS name server.

7.2.1 Name Server Software

Instruction: If in the response to Question G in *Section 4.1.1,Pre-Trip Preliminary Interview Questions,* indicates that a name server is running a DNS implementation other than BIND or Windows 2000 DNS, then this is a finding. Unless operational requirements cannot be met with these options, in which case the alternative must still be configured in a manner to satisfy the general security requirements listed in this STIG.

PDI:	DNS0400	Category:	II
MAC/Confidentiality Levels:	MAC I – CSP, MAC II – CSP, MAC III – CSP		
IA Controls:	ECMT-1, ECMT-2, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	The name server software on production name servers is not BIND or Windows 2000 DNS.		
Reference:	DNS STIG: Section 3.1		

7.2.2 Enclave Access

Instruction: Based on the answer to Question E and F in *Section 4.2.1, Network Specialist Interview Questions,* determine whether external hosts are able to query a name server on the internal network. If external hosts are able to query a name server on the internal network, then this is a finding.

PDI:	DNS0405	Category:	II
MAC/Confidentiality Levels:	MAC I – CSP, MAC II – CSP, MAC III – CSP		
IA Controls:	ECCD-1, ECCD-2, EBBD-1, EBBD-2, EBBD-3, EBPW-1		
Vulnerability Description:	Hosts outside an enclave can directly query or request a zone transfer from a name server that resides on the internal network (i.e., not in a DMZ).		
Reference:	DNS STIG: Section 3.4.3		

7.3 Console-based Checks

This section of the review covers compliance with DNS STIG requirements that cannot be determined through the questionnaires, documentation, procedures, or configuration and zone files. Rather, validation of compliance with the requirements is determined via an operating system console. An authorized SA should perform the required actions. He or she will work side-by-side with the reviewer to determine which commands are most appropriate at certain points in the review.

7.3.1 Name Server Operating System

Instruction: The operating systems and versions of these operating systems that DISA has approved to support DNS server software are:

- Sun Solaris 2.6 and above
- HP-UX 10 and above
- Windows NT 4.0
- Windows 2000 and 2003

Reviewers should check for updates to the instructions to determine if additional operating systems have been added to this list.

To determine whether a name server is supported by an approved operating system and version, the reviewer should ask the SA to run the **ver** command for Windows implementations and the **uname –a** for UNIX implementations from a command prompt. This will generate the operating system and version information. If the operating system supporting the DNS server software is not DISA approved, then this is a finding.

PDI:	DNS0410	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECMT-1, ECMT-2, ECSC-1, DCBP-1		
Vulnerability Description:	DNS server software does not run on an approved operating system.		
Reference:	DNS STIG: Section 3.2		

7.3.2 Dedicated Hardware

Instruction: During the initial interviews, the reviewer may have already identified that a name server is supporting production services other than DNS. At this point, the reviewer should validate that response through a hands-on check of the actual name server.

- UNIX

  The only permitted services to be running on a DNS UNIX BIND server are those implementing:

  - DNS
  - Secure shell
  - Host intrusion detection
  - Host file integrity
  - Network management or monitoring
  - Anti-virus
  - Backup
  - UPS

The below are not permitted:

Services started through inetd.conf:

admind, chargen, echo, etherstatd, fingerd, ftpd, httpd, ICQ server, identd, netstat, netstatd, nit, nntp, nsed, nsemntd, pfilt, portd, quaked, rexd, rexecd, rje_mapper, rlogind, rpc_3270, rpc_alias, rpc_database, rpc_keyserv, rpc_sched, rquotad, rsh, rstatd, rusersd, selectd, serverd, showfhd, sprayd, statmon, sunlink_mapper, sysstat, talkd, telnetd, tfsd, tftpd, timed, ttdb, ugidd, uucpd, and walld.

Services started at boot time:

NFS client, NFS server process and SNMP daemon, automounter, printer queue daemon, and RPC portmapper. (For Solaris, disable the following scripts in rc2.d: S73nfs.client, S74autofs, S80lp, S71rpc, and S99dtlogin and the following scripts in rc3.d: S15nfs.server and S76snmpd.)

Instruction: In the presence of the reviewer, the SA should enter the following command:

ps –ef

Based on the command output, the reviewer should be able to determine if the machine is dedicated to DNS or if it is supporting other production services. If additional services are running and it is determined the name server is not running on dedicated hardware, then this is a finding.

- Windows

The only permitted services to be running on a Windows ISC BIND DNS server are those implementing:

- DNS (i.e., the ISC BIND service) or
- DNS Server (i.e., Windows 2000 DNS)
- Host intrusion detection
- Host file integrity
- Network management or monitoring
- Anti-virus
- Backup
- UPS

Instruction: The reviewer should examine the Windows Services GUI to identify started services (in Windows 2000, right click on “My Computer” and select “Manage.” In the left windowpane, click on “Services and Applications.” A list of services is displayed in the right windowpane. Click on the “Status” column heading to sort by status. The started services will be grouped together). Also check the “Applications” tab of “Task Manager” for applications that do not run as a service. (Simultaneously press Ctrl-Alt-Del keys and select the “Applications” tab.)

Based on this examination, the reviewer should be able to determine if the machine is dedicated to DNS or if it is supporting other production services. If additional services are running and it is determined the name server is not running on dedicated hardware, then this is a finding. The exception is Windows 2000 DNS, which may run domain controllers that host Active Directory services.

PDI:	DNS0415	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		DCPA-1, ECSC-1, DCBP-1	
Vulnerability Description:		DNS software does not run on dedicated hardware.	
Reference:		DNS STIG: Section 3.2	

7.3.3 Access to Key Files

- UNIX

Instruction: The reviewer must work with the SA to obtain the user name running the *named* process.

In the presence of the reviewer, the SA should enter the following command to obtain the owner of the *named* process:

```
ps –ef  | grep named
```

In the presence of the reviewer, the SA should enter the following command while in the directory containing the DNS encryption keys:

```
ls -l
```

If the DNS encryption key files have permissions that allow read access to anyone beyond the owner of the *named* process, then this is a finding.

- Windows

Instruction: The reviewer must work with the SA to obtain the owner of the *named.exe* program.

In the presence of the reviewer, the SA should right-click on the *named.exe* file and select Properties | Security tab | Advanced | Owner tab.

For each DNS encryption key file, right-click on the file and select Properties | Security tab.

If the DNS encryption key files have permissions that allow read access to anyone beyond the owner of the *named.exe* program, then this is a finding.

PDI:	DNS0420	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECLP-1, ECCD-1, ECCD-2, ECPA-1, ECSC-1, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	File permissions on files containing DNS encryption keys are inadequate.		
Reference:	DNS STIG: Section 3.2		

7.3.4 Access to Zone Files

- UNIX

Instruction: The review must obtain the username and groupname of the DNS database administrator. The name of the DNS database administrator was obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures*. The reviewer must work with the SA to obtain the username and groupname of the DNS database administrator, DNS software administrator, and the username running the *named* daemon process.

In the presence of the reviewer, the SA should enter the following command to obtain the owner of the *named* process:

```
ps –ef | grep named
```

There are different ways (e.g., password/group file, NIS+, etc.) to obtain the DNS database administrator’s username and groupname, the reviewer is to work with the SA to obtain this information based on the configuration of the site’s UNIX OS.

In the presence of the reviewer, the SA should enter the following command while in the directory containing the zone files:

```
ls -l
```

If the zone files have permissions that allow write access to anyone beyond the owner of the *named* process or the DNS database administrator then this is a finding.

- Windows

Instruction: The review must obtain the username and groupname of the DNS database administrator. The name of the DNS database administrator was obtained in *Section 4.1.2, Pre-Trip Documentation and Procedures*. The reviewer must work with the SA to obtain the owner of the *named.exe* program.

In the presence of the reviewer, the SA should right-click on the *named.exe* file and select Properties | Security tab | Advanced | Owner tab.

For each zone file, right-click on the file and select Properties | Security tab.

If the zone files have permissions that allow write access to anyone beyond the owner of the *named.exe* program or the DNS database administrator, then this is a finding.

PDI:	DNS0425	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECLP-1, ECCD-1, ECCD-2, ECPA-1, ECSC-1, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	File permissions on DNS zone files are inadequate.		
Reference:	DNS STIG: Section 3.2		

7.3.5 Access to Configuration Files

- UNIX

Instruction: The review must obtain the user name and group name of the DNS software administrator. The name of the DNS software administrator is obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures*. The reviewer must work with the SA to obtain the username and groupname of the DNS software administrator and the username running the *named* daemon process.

In the presence of the reviewer, the SA should enter the following command to obtain the owner of the *named* process:

```
ps –ef  | grep named
```

There are different ways (i.e., password/group file, NIS+, etc.) to obtain the DNS software administrator’s username and groupname, the reviewer is to work with the SA to obtain this information based on the configuration of the site’s UNIX OS.

In the presence of the reviewer, the SA should enter the following command while in the directory containing the DNS configuration files:

```
ls -l
```

If the DNS configuration files have permissions that allow write access to anyone beyond the DNS software administrator or permissions that allow read access to anyone beyond the owner of the *named* process or the DNS software administrator then this is a finding.

- Windows

Instruction: The reviewer must obtain the username and groupname of the DNS software administrator. The name of the DNS software administrator is obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures*. The reviewer must work with the SA to obtain the username and groupname of the DNS software administrator and the owner of the named.exe program.

In the presence of the reviewer, the SA should right-click on the named.exe file and select Properties | Security tab | Advanced | Owner tab.

For each DNS configuration file, right-click on the file and select Properties | Security tab.

If the DNS configuration files have permissions that allow write access to anyone beyond the DNS software administrator or permissions that allow read access to anyone beyond the owner of the *named* process or the DNS software administrator then this is a finding.

PDI:	DNS0430	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECLP-1, ECCD-1, ECCD-2, ECPA-1, ECSC-1, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	File permissions on DNS configuration files are inadequate.		
Reference:	DNS STIG: Section 3.2		

7.3.6 Name Server's IP Address

- UNIX

Instruction: In the presence of the reviewer, the SA should enter the following command to verify the IP address is not obtained by DHCP, hme0 is used as an example, please confirm the interface:

ifconfig *hme0* auto_dhcp status

If "Ifconfig: hme0: interface is not under DHCP control," is not displayed, then this is a finding.

Please note this above mentioned command does not work on every version of UNIX, if this command does not work, please use the below instruction.

In the presence of the reviewer, the SA enters the following command while in the /etc directory: The reviewer should ensure the file */etc/dhpc.hme0* is not located on the server.

ls -l

If the file *dhcp.hme0* is listed (interface designation may different), then this is a finding.

- Windows

  Instruction: In the presence of the reviewer, the SA should select Start | Run, this will bring up the "Run" dialog box. Type **cmd** at the command line, this will bring up the command screen. Enter the following command:

  ipconfig /all

  If "DHCP Enabled" is not set to "No," then this is a finding.

PDI:	DNS0435	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		ECSC-1, DCCS-1, DCCS-2, DCBP-1	
Vulnerability Description:		The name server's IP address is not statically defined.	
Reference:		DNS STIG: Section 3.2	

7.3.7 Integrity Checking Tool

A few security tools that provide file system integrity are:

Enterprise Security Manager by Symantec	-	File system integrity and password strength
SPI-NET by LLNL	-	File system integrity and password strength
System Scanner by ISS	-	File system integrity and password strength
Tripwire by Tripwire, Inc.	-	File system integrity

- UNIX

  Instruction: The reviewer must work with the SA to obtain the program name.

  In the presence of the reviewer, the SA should enter the following command to confirm the integrity checking tool is installed and running:

  ps –ef | grep *process name*

  If an integrity checking tool is not installed and running, then this is a finding.

  With the assistance of the SA, confirm that the integrity checking tool is monitoring for any modifications to the root hints and name server's configuration (e.g., *named.conf)*, if this is not the case, then this is a finding. If using BIND name server software, common names for the root hints file are *root.hints, named.cache*, or *db.cache*. The name is configurable within the *named.conf* file.

- Windows

  Instruction: The reviewer must work with the SA to obtain the service name.

Instruction: The reviewer should examine the Windows Services GUI to identify started services (in Windows 2000, right click on "My Computer" and select "Manage". In the left windowpane, click on "Services and Applications". A list of services is displayed in the right windowpane. Click on the "Status" column heading to sort by status. The started services will be grouped together). Also check the "Applications" tab of "Task Manager" for applications that do not run as a service (Simultaneously press Ctrl-Alt-Del keys and select the "Applications" tab). The reviewer should be able to determine if an integrity checking tool is installed and running.

If an integrity checking tool is not installed and running, then this is a finding.

With the assistance of the SA, confirm that the integrity checking tool is monitoring for any modifications to the root hints and DNS configuration files (e.g., *named.conf*), if this is not the case, then this is a finding. IF using BIND name server software, common names for the root hints file are *root.hints, named.cache,* or *db.cache*. The name is configurable within the *named.conf* file.

PDI:	DNS0440	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	VIVM-1		
Vulnerability Description:	An integrity checking tool is not monitoring for any modifications to the root hints and name server configuration files.		
Reference:	DNS STIG: Section 3.2		

7.3.8 Key Files

- BIND

Instruction: With the SA's assistance, the reviewer should locate the file directory that contains the TSIG keys (i.e., */etc/dns/keys/)* and then list the files in that directory (e.g., by using the UNIX **ls –l** command). The *key* statements in *named.conf* will provide the location of the key files. If any of them have a last modified time stamp that is more than one year old, then this is a finding.

- Windows 2000 DNS

Instruction: This is not applicable to Windows 2000 DNS.

PDI:	DNS0445	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	DCCS-1, DCCS-2, ECSC-1, DCBP-1		
Vulnerability Description:	A cryptographic key used to secure DNS transactions has been utilized on a name server for more than one year.		
Reference:	DNS STIG: Sec. 7.3.2		

7.4 Checks Associated with Review of Documentation and Procedures

The documentation and procedures, obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures,* will enable the reviewer to complete this section.

Judgments as to whether the procedures are adequate should not be based on the subjective opinion of the reviewer. Rather, the reviewer should limit the review to identifying whether required elements of the procedures exist.

7.4.1 Dynamic Updates

- BIND

  Instruction: The reviewer should review the configuration files and check each zone statement for the presence of the *allow-update* phrase, which enables cryptographically authenticated dynamic updates:

  The reviewer should identify the *allow-update* phrase. The following example disables dynamic updates:

```
        allow-update {none;};
```

  If dynamic updates are not disabled, as the shown in the above example, they must be cryptographically authenticated as shown in the below example.

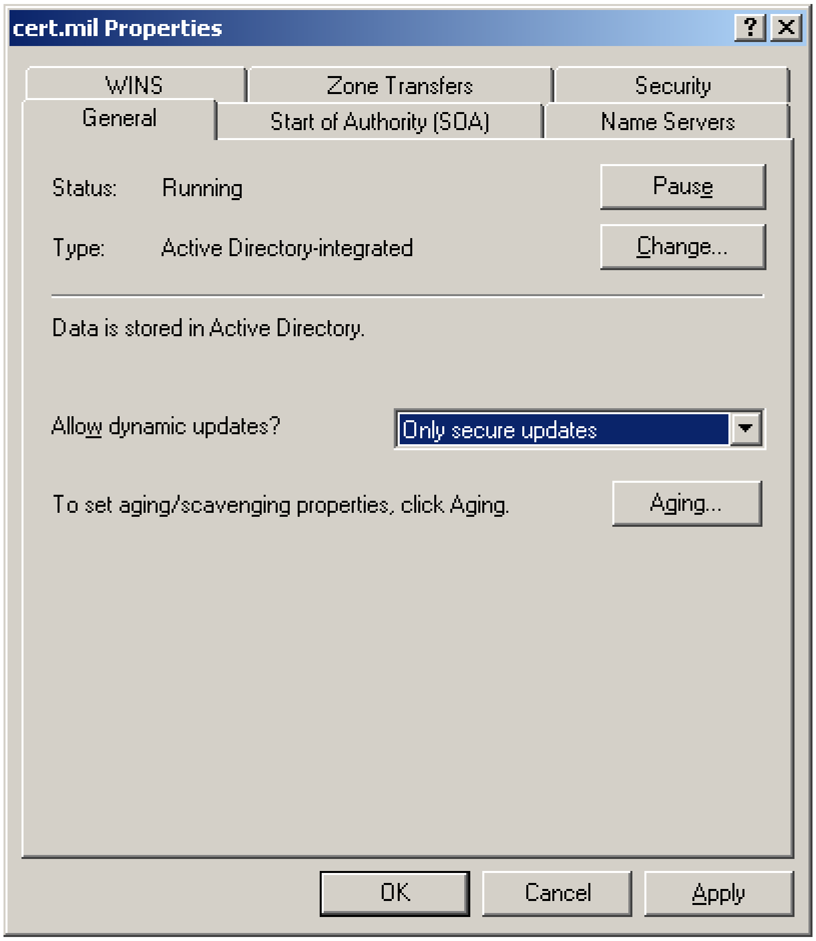
  The following example demonstrates cryptographically authenticated dynamic updates:

```
        allow-update {key
        ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil;
};
```

  If dynamic updates are not disabled or cryptographically authenticated, then this is a finding.

- Windows 2000 DNS

  Instruction: In the presence of the reviewer, the SA must review the “Properties” dialog box, select the “General” tab, and check to see if dynamic updates are allowed. If dynamic updates are enabled, ensure that “Only secure updates” has been selected. If this is not the case, then this is a finding.



Status: Running

Type: Active Directory-integrated

Data is stored in Active Directory.

Allow dynamic updates? Only secure updates

To set aging/scavenging properties, click Aging.

In cases in which the name server is not running BIND or Windows 2000 DNS, the reviewer must still examine the configuration and its documentation to validate this requirement.

PDI:	DNS0450	Category:	I
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		IAIA-1, ECSC-1, ECCD-1, ECCD-2, DCCS-1, DCCS-2, DCBP-1	
Vulnerability Description:		Dynamic updates are enabled and not cryptographically authenticated.	
Reference:		DNS STIG: Section 3.4.1.1	

7.4.2 Authenticate Master

- BIND

Instruction: This check is only applicable to slave servers, the answer to Question C in *Section 4.1.1, Pre-Trip Preliminary Interview Questions,* will indicate if the reviewed name server is a slave name server and indicate the master name server. If there is no *allow-transfer* phrase within the *zone* statement, then this is a CAT I finding. If there is an *allow-transfer* statement, there is to be a TSIG key corresponding to each of the zone partners. The reviewer can validate this by examining the *key* and *server* statements within *named.conf*. Check the *keys* phrase within each of the *server* statements. Verify the *key* statement is configured to cryptographically authenticate the master name server, an example is provided below, if this is not configured, then this is a finding. Verify the *keys* phrase is configured to cryptographically authenticate the master name server, and example is provided below, if this is not configured, then this is a finding.

On the master name server, this is an example of a configured *key* statement:

```
key ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil. {
     algorithm hmac-md5;
     include "/etc/dns/keys/tsig-example.key";
};

zone “disa.mil” {
     type master;
     file “db.disa.mil”;
     allow-transfer { key
ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil.; };
};
```

On the slave name server, this is an example of a configured key statement:

```
key ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil. {
  algorithm hmaz-,d5;
  include "/etc/dns/keys/tsig-example.key";
};

server 10.2.2.2 {
  keys {ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil};
};
```

```
zone “disa.mil” {
    type slave;
    msters { 10.1.1.1; };
    file “db.disa.mil”;
};
```

A violation of this requirement can have one of two severity levels depending upon the extent of the violation. If slaves do not authenticate master servers in any manner, then the discrepancy would be a Category I finding. If some form of authentication exists (i.e., based on IP address), but it is not based on cryptography, then the discrepancy would be a Category II finding.

- Windows 2000 DNS

  Instruction: This check only applies if the name server is a caching name server, the Windows 2000 DNS servers are to only be configured as master name servers, the answer to Question C in *Section 4.1.1, Pre-Trip Preliminary Interview Questions,* will indicate if the reviewed name server is a master name server. If the Windows 2000 DNS name server is configured as a caching name server, then this is a finding,

In cases in which the name server is not running BIND or Windows 2000 DNS, the reviewer must still examine the configuration and its documentation to validate this requirement.

PDI:	DNS0455	Category:	I-II[1]
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	IAIA-1, ECSC-1, ECCD-1, ECCD-2, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	A slave supporting a zone does not cryptographically authenticate its master before accepting zone updates.		
Reference:	DNS STIG: Section 3.4.1.2		

[1] A violation of this requirement can have one of two severity levels depending upon the extent of the violation. If slaves do not authenticate masters in any manner, then the discrepancy would be a Category I finding. If some form of authentication exists (i.e., based on IP address), but it is not based on cryptography, then the discrepancy would be a Category II finding.

7.4.3 Authentication of Zone Transfers

- BIND

  Instruction: This check is only applicable to zone master servers, the answer to Question C in *Section 4.1.1, Pre-Trip Preliminary Interview Questions,* will indicate if the reviewed name server is a master name server. If there are no *allow-transfer* phrases within *named.conf*, then this is a finding. If there are *allow-transfer* phrases, then check that there is one corresponding to each of the zone partners listed in the response to Question C in *Section 4.1.1, Pre-Trip Preliminary Interview Questions*. If this is not the case, then this is also a finding.

  If there are *allow-transfer* phrases for servers other than those supplied, then there may be a finding associated with the incompleteness of the list.

  If the *key* statement references a file, then no other *key* statement should reference the same file.

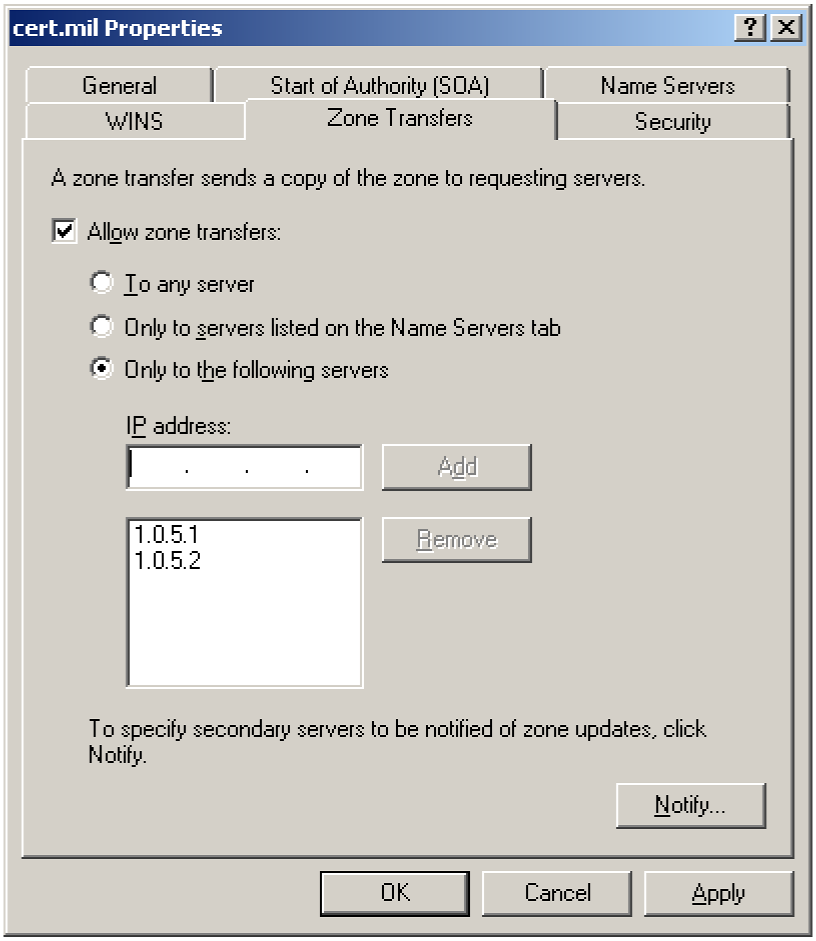
  If the *key* statement includes a character representation of the key itself (an improper configuration), then no other *key* statement should include the same character string.

  On the master name server, this is an example of a configured *allow-transfer* phrase:

```
  zone “disa.mil” {
    type master;
    file “db.disa.mil”;
    allow-transfer { key
  ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil.; };
};
```

- Windows 2000 DNS

  If “Allow zone transfers:” is checked, “Only to the following servers” is to be also checked. The reviewer must validate the name servers listed based on Question C in *Section 4.1.1, Pre-Trip Preliminary Interview Questions*. If this is not the case, then this is a finding.
  An example of a compliant server is shown below:



A zone transfer sends a copy of the zone to requesting servers.

☑ Allow zone transfers:

○ To any server

○ Only to servers listed on the Name Servers tab

● Only to the following servers

IP address:

1.0.5.1
1.0.5.2

To specify secondary servers to be notified of zone updates, click Notify.

In cases in which the name server is not running BIND or Windows 2000 DNS, the reviewer must still examine the configuration and its documentation to validate this requirement.

PDI:	DNS0460	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	IAIA-1, ECSC-1, ECCD-1, ECCD-2, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	A zone master server does not limit zone transfers to a list of active slaves authoritative for that zone.		
Reference:	DNS STIG: Section 3.4.1.2		

7.4.4 TSIG Zone Transfers

Instruction: This check is only applicable to master name servers, the answer to Question C in *Section 4.1.1, Pre-Trip Preliminary Interview Questions*, will indicate if the reviewed name server is a master name server and a list of the slave name servers. If there is no *allow-transfer* phrase within the *options* or *zone* statement, this is a finding. If there is an *allow-transfer* statement, there is to be a TSIG key corresponding to each of the zone partners. The reviewer can validate this by examining the *key* and *server* statements within *named.conf*. If the TSIG key of any other host is included in this phrase, then this is a finding.

On the master name server, this is an example of a configured *key* statement:

```
     key ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil. {
          algorithm hmac-md5;
          include "/etc/dns/keys/tsig-example.key";
     };

     zone “disa.mil” {
          type master;
          file “db.disa.mil”;
          allow-transfer { key
     ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil.; };
     };
```

On the slave name server, this is an example of a configured *key* statement:

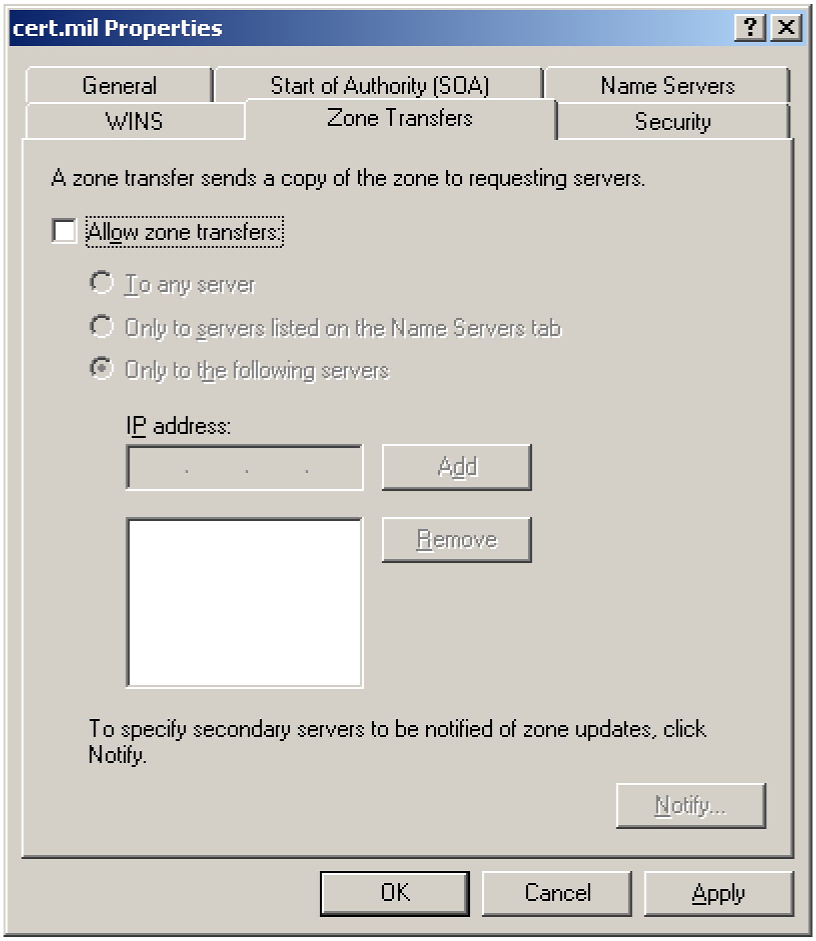
```
     key ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil. {
          algorithm hmac-md5;
          include "/etc/dns/keys/tsig-example.key";
     };

     server 10.2.2.2 {
               keys
     {ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil};
     };

     zone “disa.mil” {
          type slave;
          masters { 10.1.1.1; };
          file “db.disa.mil”;
   };
```

- Windows 2000 DNS

  Instruction: If “Allow zone transfers:” is checked, then this is a finding. An example of a compliant server is shown below:



A zone transfer sends a copy of the zone to requesting servers.

☐ Allow zone transfers:

○ To any server

○ Only to servers listed on the Name Servers tab

● Only to the following servers

IP address:

To specify secondary servers to be notified of zone updates, click Notify.

In cases in which the name server is not running BIND or Windows 2000 DNS, the reviewer must still examine the configuration and its documentation to validate this requirement.

PDI:	DNS0465	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	IAIA-1, ECSC-1, ECCD-1, ECCD-2, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	A zone master server does not cryptographically authenticate slaves requesting a zone transfer.		
Reference:	DNS STIG: Section 3.4.1.2		

7.4.5 Notifies

- BIND

  Instruction: If all of a zone's NS records are valid, then the default behavior in BIND complies with this requirement and does not require the DNS software administrator to take any additional action.

  In some cases, the DNS software administrator must implement a non-default configuration to comply with operation requirements. If this is the case, the DNS software administrator must have an understanding of the *named.conf* options that govern how master name servers notify other hosts of zone changes and when slave servers will accept notifications. If none of these options are selected, the resulting behavior represents an acceptable security risk. If these phrases are configured, then this is a finding.

  The three phrases within the *options* statement that govern this behavior are:

  - *notify* – which turns notification on or off (defaults to on)

  - *also-notify* – which defines servers other than those listed in NS records that will be sent notifications (defaults to none)

  - *allow-notify* – which defines from which servers a slave will accept notifications (defaults to the master name server only)

- Windows 2000 DNS

  Instruction: This check only applies if the name server is a caching name server, the Windows 2000 DNS servers are to only be configured as master name servers, the answer to Question C in *Section 4.1.1, Pre-Trip Preliminary Interview Questions*, will indicate if the reviewed name server is a master name server. If the Windows 2000 DNS name server is configured as a caching name server, then this is a finding.

In cases in which the name server is not running BIND or Windows 2000 DNS, the reviewer must still examine the configuration and its documentation to validate this requirement.

PDI:	DNS0470	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		IAIA-1, ECSC-1, ECCD-1, ECCD-2, DCCS-1, DCCS-2, DCBP-1	
Vulnerability Description:		A name server is not configured to only accept notifications of zone changes from a host authoritative for that zone.	
Reference:		DNS STIG: Section 3.4.1.2	

7.4.6 Recursion – Master Name Server

- BIND

  Instruction: This check only applies if the name server is a master name server, the answer to Question C in *Section 4.1.1, Pre-Trip Preliminary Interview Questions,* will indicate if the reviewed name server is a master name server.

  The reviewer should identify the *recursion* and *allow-query* phrases. They should look as follows:

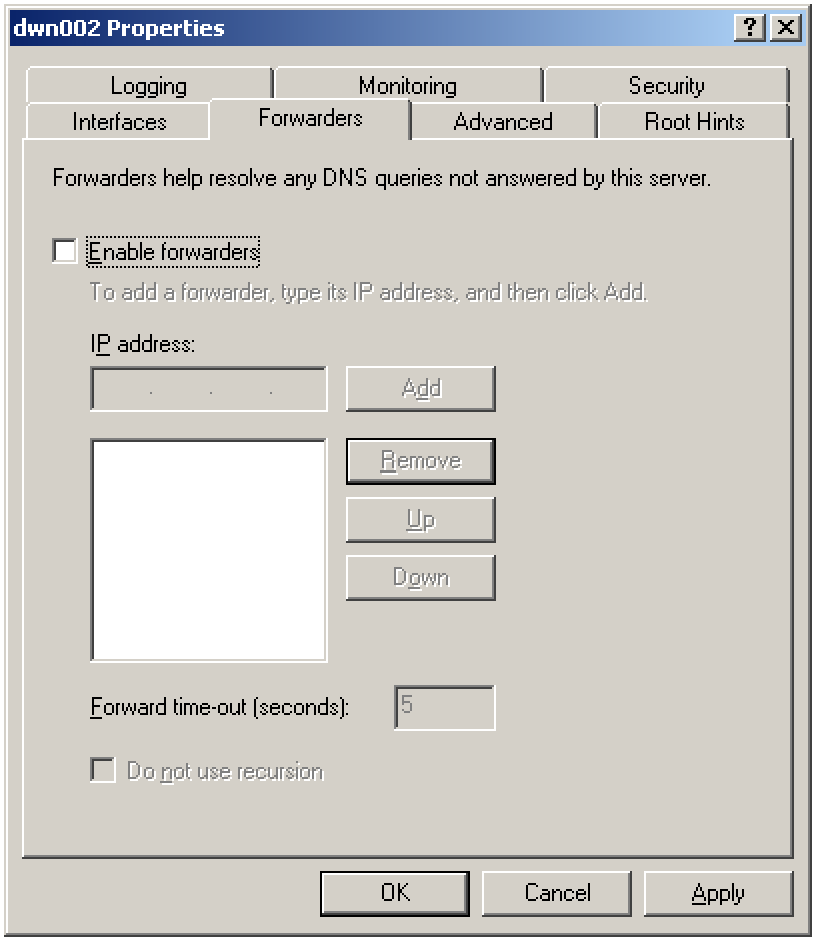
  ```
  recursion no;
      allow-query {none;};
  ```

  If either of these phrases is either missing or has a value other than what is listed above, then this is a finding.

- Windows 2000 DNS

  Instruction: This check only applies if the name server is a master name server, the Windows 2000 DNS servers are to only be configured as master name servers, the answer to Question C in *Section 4.1.1*, *Pre-Trip Preliminary Interview Questions*, will indicate if the reviewed name server is a master name server.

  If “Enable forwarders” is checked, this constitutes a finding. An example of a compliant server is shown below:



dwn002 Properties

Forwarders help resolve any DNS queries not answered by this server.

☐ Enable forwarders

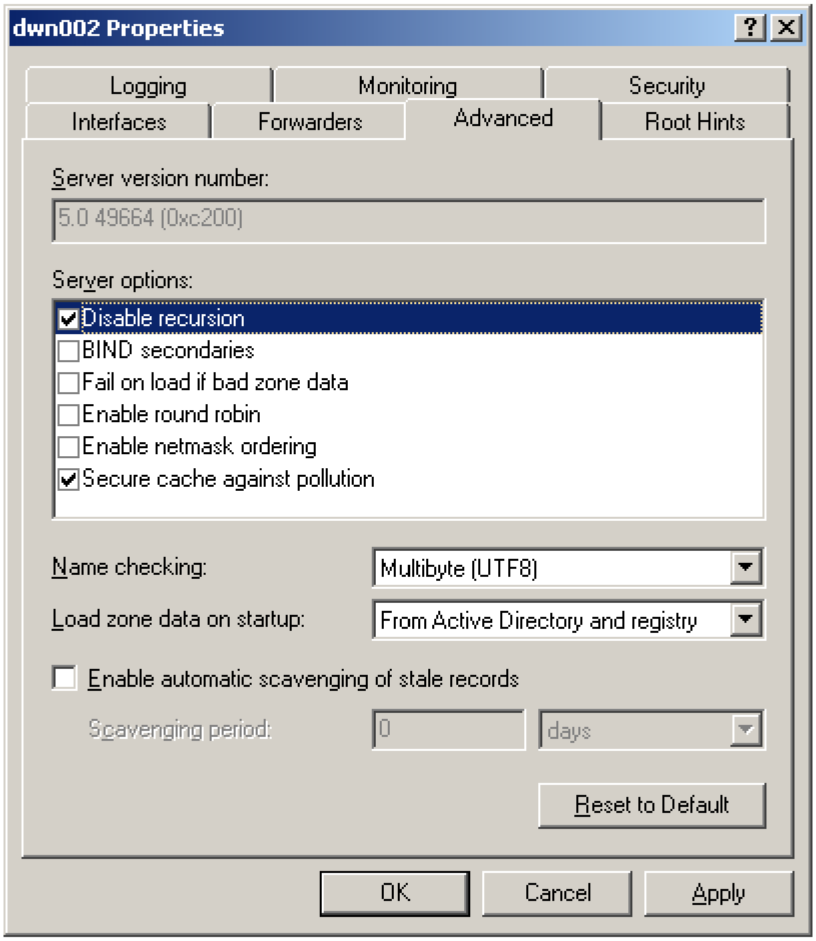
To add a forwarder, type its IP address, and then click Add.

IP address:

Forward time-out (seconds): 5

☐ Do not use recursion

Also examine the “Advanced” tab of the DNS Server “Properties” dialog box. If “Disable recursion” is not checked, then this is a finding. An example of a compliant server is shown below:



dwn002 Properties

Server version number: 5.0 49664 (0xc200)

Server options:

☑ Disable recursion
☐ BIND secondaries
☐ Fail on load if bad zone data
☐ Enable round robin
☐ Enable netmask ordering
☑ Secure cache against pollution

Name checking: Multibyte (UTF8)

Load zone data on startup: From Active Directory and registry

☐ Enable automatic scavenging of stale records

Scavenging period: 0 days

In cases in which the name server is not running BIND or Windows 2000 DNS, the reviewer must still examine the configuration and its documentation to validate this requirement.

PDI:	DNS0475	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECSC-1, ECCD-1, ECCD-2, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	Recursion is not prohibited on an authoritative name server.		
Reference:	DNS STIG: Section 3.4.2.2		

7.4.7 Recursion – Caching Name Server

- BIND

Instruction: This check is only applicable to caching name servers, the answer to Question C in *Section 4.1.1, Pre-Trip Preliminary Interview Questions,* indicate if the reviewed name server is a caching name server. The reviewer should have learned the internal IP address ranges in the answer to Question A in *Section 4.2.1, Network Specialist Interview Questions*. Verify the *allow-query* and *allow-recursion* phrases are properly configured.

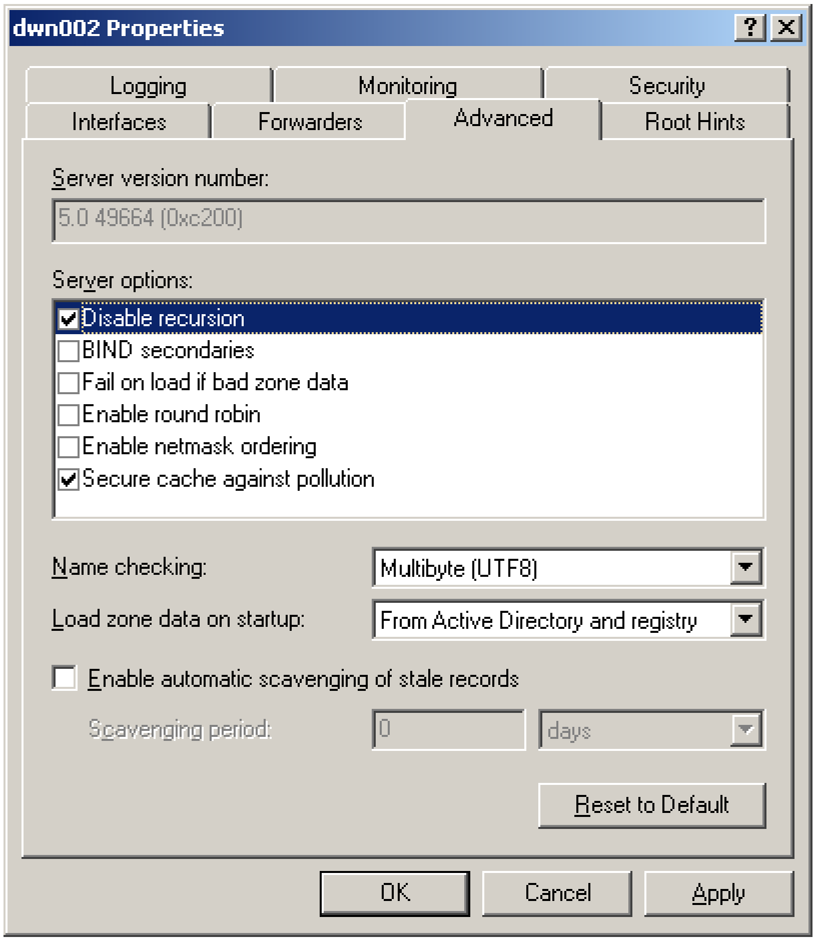
The reviewer should identify the *allow-query* and *allow-recursion* phrases. It should look as follows:

```
allow-query {trustworthy_hosts;};
allow-recursion {trustworthy_hosts;};
```

The name of the ACL does not need to be “trustworthy_hosts” but the name should match the ACL name defined earlier in *named.conf* for this purpose. If not, then this is a finding. The reviewer will also check for whether non-internal IP addresses appear in either the referenced ACL (e.g., trustworthy_hosts) or directly in the statements themselves. If non-internal IP addresses do appear, then this is a finding.

- Windows 2000 DNS

  Instruction: Windows 2000 DNS should not be deployed as a caching name server. Consequently, the use of forwarders and recursion is prohibited on Windows 2000 DNS. The reviewer will validate that the "Disable recursion" and the “Secure cache against pollution" on the “Advanced” tab of the name server properties are selected. Examine the “Advanced” tab of the DNS Server “Properties” dialog box. If “Disable recursion” and “Secure cache against pollution” is not checked, then this is a finding. An example of a compliant server is shown below:



dwn002 Properties

Server version number: 5.0 49664 (0xc200)

Server options:

☑ Disable recursion
☐ BIND secondaries
☐ Fail on load if bad zone data
☐ Enable round robin
☐ Enable netmask ordering
☑ Secure cache against pollution

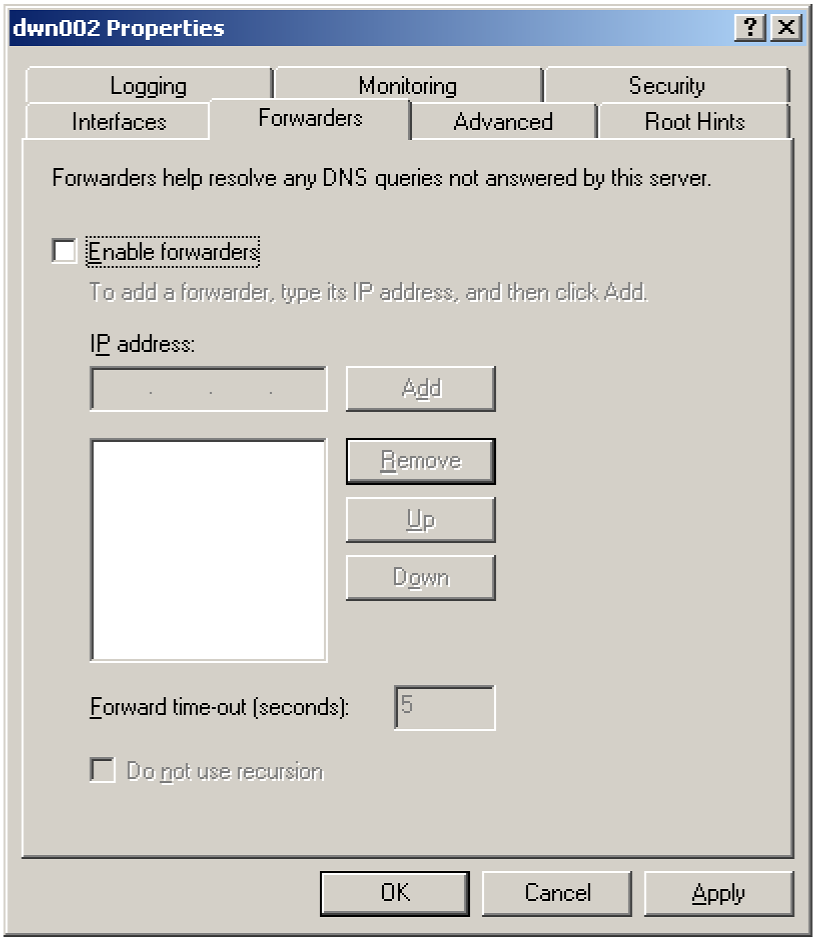
Name checking: Multibyte (UTF8)

Load zone data on startup: From Active Directory and registry

☐ Enable automatic scavenging of stale records

Scavenging period: 0 days

The reviewer will also validate that the "Enable forwarders" on the “Forwarders” tab of the name server properties is not selected. Examine the “Forwarders” tab of the DNS Server “Properties” dialog box. If “Enable forwarders” is checked, then this is a finding. An example of a compliant server is shown below:



Forwarders help resolve any DNS queries not answered by this server.

☐ Enable forwarders

To add a forwarder, type its IP address, and then click Add.

IP address: . . .

Forward time-out (seconds): 5

☐ Do not use recursion

In cases in which the name server is not running BIND or Windows 2000 DNS, the reviewer must still examine the configuration and its documentation to validate this requirement.

PDI:	DNS0480	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	IAIA-1, ECSC-1, ECCD-1, ECCD-2, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	A caching name server does not restrict recursive queries to only the IP addresses and IP address ranges of known supported clients.		
Reference:	DNS STIG: Section 3.4.2.2		

7.4.8 Logging Events

DNS software administrators need DNS transaction logs for a wide variety of reasons including troubleshooting, intrusion detection, and forensics. The events the name server logs are to contain, at a minimum, success and failure of the following events:

- start and stop of the name server service or daemon
- zone transfers
- zone update notifications

- queries
- dynamic updates

- BIND

Instruction: For a BIND configuration: if a *logging* statement is present, it will have the form:

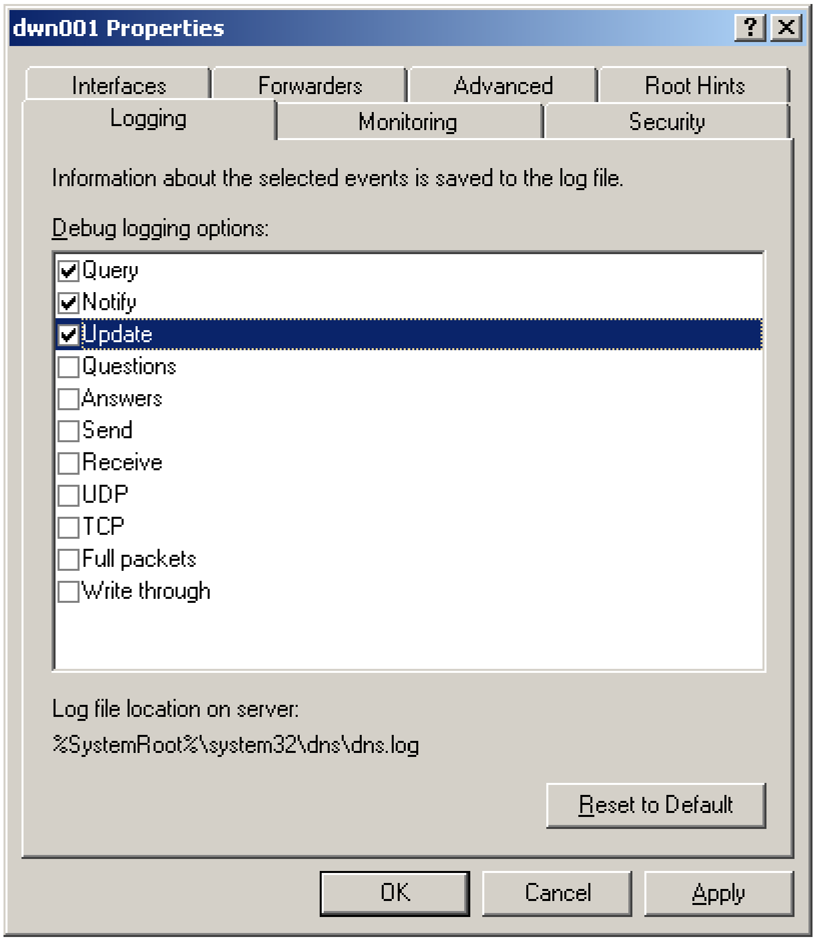
```
logging {
     channel channel_name
          file path_name | syslog syslog_facility
          severity (critical | error | warning |
               notice | info | debug [level]| dynamic);]
               print-severity yes/no;
               print-time yes/no;
     };

     category category_name {
          channel_name ; [ channel_name ; …
          };
};
```

Instruction: If a *logging* statement is not present, then this is a finding. The reviewer will look at the severity clause in each of the *channel* phrases of the *logging* statement. It should read either notice, info or debug for each defined channel (although debug would not typically appear unless the review is concurrent with a troubleshooting effort). If the *logging* statement is not properly configured, then this is a finding.

- Windows 2000 DNS

Instruction: For a Windows 2000 DNS configuration: On the “Logging Tab” of the “DNS Server Properties” dialog box, if “Query”, “Notify”, and “Update” are not checked in the “Debug Logging” options, then this is a finding. An example of a compliant server is shown below:



Information about the selected events is saved to the log file.

Debug logging options:

- ☑ Query
- ☑ Notify
- ☑ Update
- ☐ Questions
- ☐ Answers
- ☐ Send
- ☐ Receive
- ☐ UDP
- ☐ TCP
- ☐ Full packets
- ☐ Write through

Log file location on server:
%SystemRoot%\system32\dns\dns.log

In cases in which the name server is not running BIND or Windows 2000 DNS, the reviewer must still examine the configuration and its documentation to validate this requirement.

PDI:	DNS0485	Category:	I-II[2]
MAC/Confidentiality Levels:	MAC I – CSP, MAC II – CSP, MAC III – CSP		
IA Controls:	ECAR-1, ECAR-2, ECAR-3, ECSC-1, DCCS-1, DCCS-2		
Vulnerability Description:	Name server logging is inadequate.		
Reference:	DNS STIG: Section 3.5		

7.4.9 Logging Facility

DNS software administrators need DNS transaction logs for a wide variety of reasons including troubleshooting, intrusion detection, and forensics. These logs should be appropriately secured, having file permissions that restrict unauthorized changes or viewing, and archived, being appropriately backed-up and stored so that they can be examined at a future time.

[2] A violation of this requirement can have one of two severity levels depending upon the extent of the violation. If no logging exists, then the discrepancy would be a Category I finding. If some logging exists, but not for all of the events listed, then the discrepancy would be a Category II finding.

- BIND

  The DNS software administrator will configure the DNS software to send all log data to either the system logging facility (e.g., UNIX syslog or Windows Application Event Log) or an alternative logging facility with security configuration equivalent to or more restrictive than the system logging facility.

  Instruction: On an examination of the DNS configuration file (if BIND, *named.conf*), the reviewer can determine whether log data is sent to a facility other than the system logging facility. If this is the case, then the reviewer should do the following at a minimum:

  - Compare the file permissions of the operating system logs with the file permissions of the alternative logging facility for DNS (e.g., using **ls –l**). If the permissions on the alternative are weaker in any manner, this constitutes a finding.

  - Determine whether the system logs are transferred or copied to media on another machine (e.g., a cron job that periodically moves logs to another computer). If this is the case and there is not a similar technology in place for the DNS logs, then this constitutes a finding.

  The reviewer can identify other ways in which the security of the DNS logs may be weaker than the security of the system logs, and can generate a finding based on that discovery so long as the explanation of the weakness is clearly documented in the SRR results.

- Windows 2000 DNS

  Windows 2000 DNS software log files will be equivalent to the system logging facility by default.

In cases in which the name server is not running BIND or Windows 2000 DNS, the reviewer must still examine the configuration and its documentation to validate this requirement.

PDI:	DNS0490	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECSC-1, ECCD-1, ECCD-2, DCBP-1		
Vulnerability Description:	Name server logs are not adequately secured.		
Reference:	DNS STIG: Section 3.5		

7.4.10 Logging Timestamps

- BIND

Instruction: Based on the *logging* statement in *named.conf*, the reviewer can determine where the DNS logs are located. If there logging is not configured, then this is a finding. These logs (which in many cases are likely to be the system logs), should be viewed using the UNIX **cat** or **tail** commands, a text editor, or – in the case of Windows – the "Event Viewer." When examining the logs, the reviewer should ensure that entries have timestamps and severity codes. If timestamps and severity codes are not found on one or more entries, then this is a finding.

```
logging {
          channel channel_name
               file path_name | syslog syslog_facility
               severity (critical | error | warning |
                 notice | info | debug [level]| dynamic);]
               print-severity yes/no;
               print-time yes/no;
          };
          category category_name {
               channel_name ; [ channel_name ; …
          };
     };
```

Instruction: If the DNS entries in the logs do not note their severity (i.e., *critical, error, warning, notice*, or *info*), then this constitutes a finding.

- Windows 2000 DNS

Windows 2000 DNS software adds timestamps and severity information by default.

In cases in which the name server is not running BIND or Windows 2000 DNS, the reviewer must still examine the configuration and its documentation to validate this requirement.

PDI:	DNS0495	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECAR-1, ECAR-2, ECAR-3, ECSC-1, DCCS-1, DCCS-2		
Vulnerability Description:	Entries in the name server logs do not contain timestamps and severity information.		
Reference:	DNS STIG: Section 3.5		

7.4.11 Root Zone File

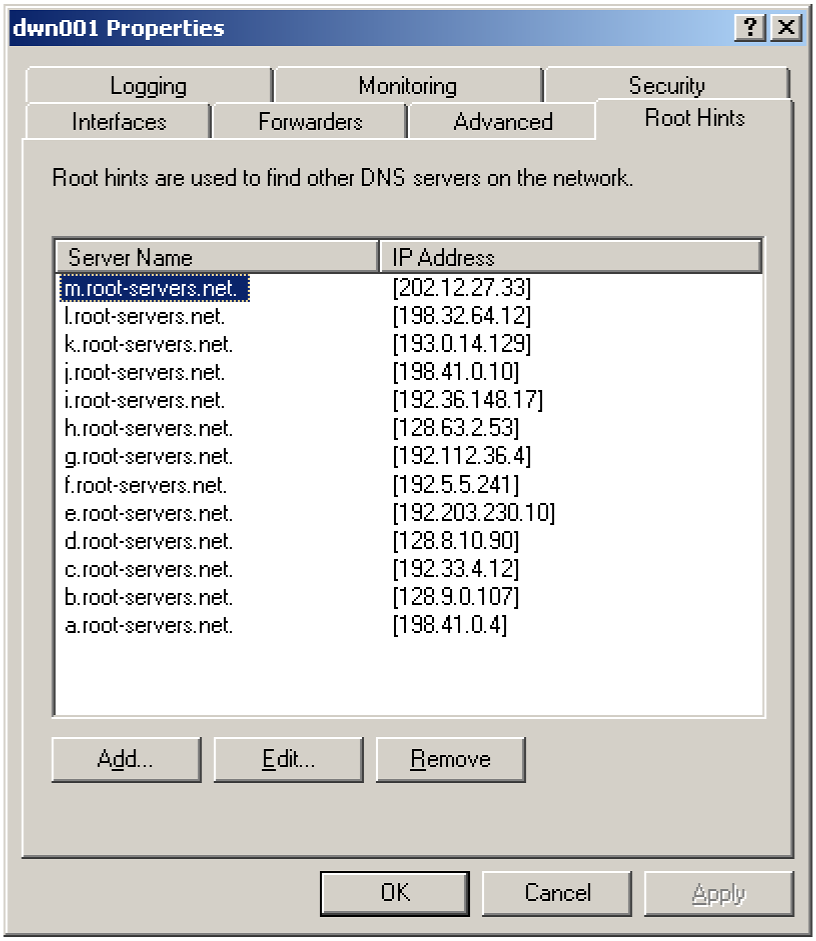
- BIND

Instruction: This check is only applicable to caching name servers, the answer to Question C in *Section 4.1.1, Pre-Trip Preliminary Interview Questions,* indicate if the reviewed name server is a caching name server. Review the entries within the root hints file and validate that the entries are correct. Common names for the root hints file are *root.hints, named.cache,* or *db.cache*. The name is configurable within the *named.conf* file. The correct entries should be:

Root Server	IP Address
A	198.41.0.4
B	128.9.0.107
C	192.33.4.12
D	128.8.10.90
E	192.203.230.10
F	192.5.5.241
G	192.112.36.4
H	128.63.2.53
I	192.36.148.17
J	192.58.128.30
K	193.0.14.129
L	198.32.64.12
M	202.12.27.33

- Windows 2000 DNS

Instruction: This check only applies if the name server is a caching name server, the Windows 2000 DNS servers are to only be configured as master name servers, the answer to Question C in *Section 4.1.1, Pre-Trip Preliminary Interview Questions,* will indicate if the reviewed name server is a master name server. This requirement is only valid if the Windows 2000 DNS server is configured as a caching server. An example of valid root hints is shown below:



Root hints are used to find other DNS servers on the network.

Server Name	IP Address
m.root-servers.net.	[202.12.27.33]
l.root-servers.net.	[198.32.64.12]
k.root-servers.net.	[193.0.14.129]
j.root-servers.net.	[198.41.0.10]
i.root-servers.net.	[192.36.148.17]
h.root-servers.net.	[128.63.2.53]
g.root-servers.net.	[192.112.36.4]
f.root-servers.net.	[192.5.5.241]
e.root-servers.net.	[192.203.230.10]
d.root-servers.net.	[128.8.10.90]
c.root-servers.net.	[192.33.4.12]
b.root-servers.net.	[128.9.0.107]
a.root-servers.net.	[198.41.0.4]

In cases in which the name server is not running BIND or Windows 2000 DNS, the reviewer must still examine the configuration and its documentation to validate this requirement.

PDI:	DNS0500	Category:	I
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	DCCS-1, DCCS-2, ECSC-1, DCBP-1		
Vulnerability Description:	The local root zone file contains an invalid root name server entry.		
Reference:	DNS STIG: Section 3.6.4		

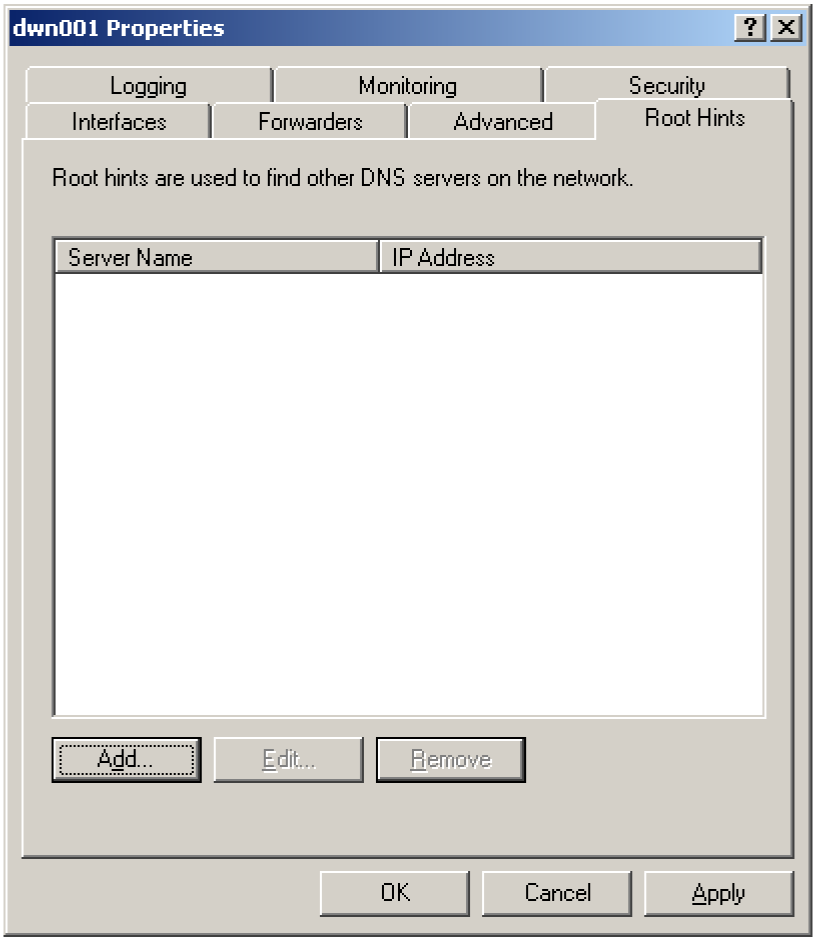
7.4.12 Root Hints

- BIND

  Instruction: This check only applies if the name server is an authoritative name server, which the reviewer should know based on the answer to Question C in *Section 4.1.1, Pre-Trip Preliminary Interview Questions*. Ensure there is not a root hints on the name server. Common names for the root hints file are *root.hints*, *named.cache*, or *db.cache*. The name is configurable within the *named.conf* file.

- Windows 2000 DNS

  Instruction: This check only applies if the name server is an authoritative name server, which the reviewer should know based on the answer to Question C in *Section 4.1.1, Pre-Trip Preliminary Interview Questions*. For a Windows 2000 DNS configuration: Select the "Root Hints" Tab of the "DNS Server Properties" dialog box, ensure the root name server entries have been removed. To remove entries, right click the entry and click the "Remove" button. An example of a compliant authoritative server is shown below:



Root hints are used to find other DNS servers on the network.

Server Name	IP Address

In cases in which the name server is not running BIND or Windows 2000 DNS, the reviewer must still examine the configuration and its documentation to validate this requirement.

PDI:	DNS0505	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	DCCS-1, DCCS-2, ECSC-1, DCBP-1		
Vulnerability Description:	The root hints file on an authoritative name server is not deleted.		
Reference:	DNS STIG: Section 3.6.4		

This page is intentionally left blank.

8. BIND NAME SERVER CONFIGURATION

This section will encompass each BIND instance, regardless of the platform of the name server and is applicable for all BIND instances. This is in addition to the Name Server Security Requirements and is to be used for each and every instance of BIND located at the site to be reviewed. This section is independent of any particular DNS architecture or platform on which BIND is configured. This addresses security requirements related to all BIND implementations regardless of the operating system, which it is running on.

The DNS SRR begins by completing the *Section 4.1, The Pre-Trip Preliminary Interview*, which includes obtaining answers to questions and gathering written documentation and procedures, and configuration and zone files prior to the onsite visit. In addition to the pre-trip information gathered, an SA will be required to assist in the console-based checks.

8.1 Vulnerabilities

Complete this entire form for each BIND instance being reviewed. For each PDI/VUL, check whether it is a finding or not a finding in the “Status” column. In cases in which the PDI/VUL is not applicable, check “Not Applicable” (e.g., it applies to an authoritative server, but you are reviewing a caching server). If a PDI/VUL is relevant to the environment, but you are unable to evaluate it for whatever reason (e.g., access restrictions or time limitations), then check “Not Reviewed.”

8.1.1 Console-based Checks

Procedure Section Headings		**Finding Information**			**PDI/VUL Information**		
Manual	**Script**	**Status**	**Details**		**PDI/VUL**	**Description**	**Cat.**
8.2.1		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0700 V0004498	A BIND name server is not running version BIND 8.2.7 or above, 8.3.4 or above, or 9.2.1 or above.	2

8.1.2 Checks Associated with Review of Documentation and Procedures

Procedure Section Headings		**Finding Information**			**PDI/VUL Information**		
Manual	**Script**	**Status**	**Details**		**PDI/VUL**	**Description**	**Cat.**
8.3.1		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0705 V0004493	A TSIG key is not correctly specified.	3
8.3.2		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0710 V0004494	A TSIG key is not in it’s own dedicated file.	2
8.3.3		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0715 V0004511	A name server accepts control messages without adequate authentication.	2

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	Script	Status	Details		PDI/VUL	Description	Cat.
8.3.4		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0720 V0004495	A unique TSIG key is not utilized for communication between name servers sharing zone information.	2
8.3.5.1		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0725 V0004496	BIND is configured to disclose its version number to queries.	3
8.3.5.2		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0730 V0004497	The named.conf options statement includes the phrase "fake-iquery yes;".	3
8.3.5.3		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0735 V0004499	The named.conf options statement includes the phrase "rfc2308-type1 yes;”.	2

8.1.3 IAVM Compliance

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	**Script**	**Status**	**Details**		**PDI/VUL**	**Description**	**Cat.**
8.4		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS8010 V0004502	IAVM notice, 2000-B-0001, has not been responded to.	1
8.4		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS8020 V0004504	IAVM notice, 2000-B-0008, has not been responded to.	1
8.4		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS8030 V0003674	IAVM notice, 2001-A-0001, has not been responded to.	1
8.4		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS8040 V0003675	IAVM notice, 2002-A-0006, has not been responded to.	1
8.4		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS8050 V0003676	IAVM notice, 2002-T-0010, has not been responded to.	1
8.4		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS8060 V0003677	IAVM notice, 2003-B-0001 has not been responded to.	1

8.2 Console-based Checks

This section of the review covers compliance with DNS STIG requirements that cannot be determined through the questionnaires, documentation, procedures, or configuration and zone files. Rather, validation of compliance with the requirements is determined via an operating system console. An authorized SA should perform the required actions. He or she will work side-by-side with the reviewer to determine which commands are most appropriate at certain points in the review.

8.2.1 BIND Version

- UNIX

  Instruction: In the presence of the reviewer, the SA should enter the following command:

  named –v

  or,

  what /usr/sbin/named | grep named

  If a version of BIND prior to 9.2.6, 9.3.1, or 8.4.7 is running, then this is a finding. If subsequent IAVA guidance recommends a BIND upgrade, then that guidance will supersede this requirement.

- Windows

  Instruction: The reviewer must work with the SA to obtain the owner of the *named.exe* service.

  In the presence of the reviewer, the SA should right-click on the *named.exe service* name file and select Properties | Version tab.

  The version should be displayed in the “Description” field.

  If a version of BIND prior to 9.2.6, 9.3.1, or 8.4.7 is running, then this is a finding. If subsequent IAVA guidance recommends a BIND upgrade, then that guidance will supersede this requirement.

PDI:	DNS0700	Category:	II
MAC/Confidentiality Levels:	MAC I – CSP, MAC II – CSP, MAC III – CSP		
IA Controls:	DCSQ-1, ECSC-1,ECMT-1, ECMT-2, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	A BIND name server is not running version BIND 9.3.1 or above, 8.4.7 or above, or 9.2.6 or above.		
Reference:	DNS STIG: Section 4.1		

8.3 Checks Associated with Review of Documentation and Procedures

The *named conf* file obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures,* will enable the reviewer to complete this section.

Judgments as to whether the procedures are adequate should not be based on the subjective opinion of the reviewer. Rather, the reviewer should limit the review to identifying whether required elements of the procedures exist.

8.3.1 The key Statement – HMAC-MD5

Instruction: There is to be a properly configured *key* statement located in the *named.conf* file obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures*. As of the release of this checklist, BIND only supports the HMAC-MD5 algorithm for TSIG. As a result, there should not be a finding for the use of HMAC-MD5 on BIND servers at this time.

When a future release of BIND supports HMAC-SHA1, organizations will be required to migrate to this algorithm and there will be an SRR finding if it is not used.

An example of a properly configured *key* statement in practice might be:

```
key ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil {
     algorithm hmac-md5;
     include “/etc/dns/keys/ns1_ns2.key”;
};
```

If the *key* statement is not configured, then this is a finding.

If the *key* statement is not configured to implement HMAC-MD5, then this is a finding.

PDI:	DNS0705	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	DCNR-1, ECSC-1, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	A TSIG key is not correctly specified.		
Reference:	DNS STIG: Section 4.2.1		

8.3.2 The key Statement – Dedicated File

Instruction: If the *key* statement includes a secret phrase followed by a character representation of the key, then this is a finding. The *key* statement is located in the *named.conf* obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures*. The correct configuration calls for an *include* statement embedded in the *key* statement. The *include* statement references a separate file that contains the key so it does not need to appear in the *named.conf* file.

An example of a properly configured *key* statement in practice might be:

```
key ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil {
     algorithm hmac-md5;
     include “/etc/dns/keys/ns1_ns2.key”;
};
```

If each key is not located in a dedicated file for each individual key, then this is a finding.

PDI:	DNS0710	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECLP-1, ECCD-1, ECCD-2, ECSC-1, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	A TSIG key is not in its own dedicated file.		
Reference:	DNS STIG: Section 4.2.1		

8.3.3 The controls Statement

Instruction: If control messages are utilized, there is to be a properly configured *keys* statement within the *controls* statement located in the *named.conf* obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures*.

An example of a properly configured *controls* statement in practice might be:

```
controls {
          inet 127.0.0.1
          allow 127.0.0.1
          keys { “rndc_key” };
};
```

If controls messages are utilized and not cryptographically authenticated, then this is a finding.

PDI:	DNS0715	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECLP-1, ECCD-1, ECCD-2, ECSC-1, DCCS-1, DCCS-2, DCBP-1		
Vulnerability	A name server accepts control messages without adequate		

Description:	authentication.
Reference:	DNS STIG: Section 4.2.2

8.3.4 The server Statement

Two name servers sharing zone information must utilize a unique TSIG key for communication between them or, in cases in which more than four servers support a zone, create a written key management plan that will document how keys are shared and replaced in a manner to reduce residual risk to an acceptable level.

Instruction: If there are no *server* statements within *named.conf* obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures*, this is a finding. If there are *server* statements, then check that there is one corresponding to each of the zone partners listed in the response to Question C in *Section 4.1.1, Pre-Trip Preliminary Interview Questions*. If this is not the case, then this is also a finding.

If there are *server* statements for servers other than those supplied, then there may be a finding associated with the incompleteness of the list.

On the master name server, this is an example of a configured *key* statement:

```
     key ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil. {
          algorithm hmac-md5;
          include "/etc/dns/keys/tsig-example.key";
     };

     zone “disa.mil” {
          type master;
          file “db.disa.mil”;
          allow-transfer { key
     ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil.; };
     };
```

On the slave name server, this is an example of a configured *key* statement:

```
     key ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil. {
          algorithm hmac-md5;
          include "/etc/dns/keys/tsig-example.key";
     };
```

```
server 10.2.2.2 {
          keys
{ns1.kalamazoo.disa.mil_ns2.kalamazoo.disa.mil};
};

zone “disa.mil” {
     type slave;
     masters { 10.1.1.1; };
     file “db.disa.mil”;
    };
```

Check the *keys* phrase within each of the *server* statements to ensure uniqueness of keys. If two or more *server* statements reference the same key, then this is a finding.

PDI:	DNS0720	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECLP-1, ECCD-1, ECCD-2, ECSC-1, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	A unique TSIG key is not utilized for communication between name servers sharing zone information.		
Reference:	DNS STIG: Section 4.2.3		

8.3.5 The options Statement

The *options* statement in the *named.conf* file defines global options for BIND. Some options can also be defined for each zone. Not all options impact security. The relevant BIND options for the DNS STIG are reviewed in this section.

8.3.5.1 The version Phrase

Instruction: Review the *named.conf* file, obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures.* The reviewer should identify the *version* phrase in the *options* statement. If it is missing, then the reviewer must generate a finding. If it is present, then it must not reveal actual version information, if this is not the case, then this is a finding.

Examples of satisfactory *version* phrases include:

```
options {
          version " ";
          [ … ]
};
```

or

```
options {
          version " version not disclosed";
          [ … ]
};
```

PDI:	DNS0725	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	DCCS-1, DCCS-2, ECSC-1, DCBP-1		
Vulnerability Description:	BIND is configured to disclose its version number to queries.		
Reference:	DNS STIG: Section 4.2.6.1		

8.3.5.2 The fake-iquery Phrase

Instruction: Review the *named.conf* file, obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures.* If the phrase “fake-iquery yes;” appears in the *options* statement, then this is a finding.

PDI:	DNS0730	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	DCCS-1, DCCS-2, ECSC-1, DCBP-1		
Vulnerability Description:	The named.conf options statement includes the phrase "fake-iquery yes;".		
Reference:	DNS STIG: Section 4.2.6.4		

8.3.5.3 The rfc2308-type1 Phrase

Instruction: Review the *named.conf* file, obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures.* If the phrase “rfc2308-type1 yes;” appears in the *options* statement, then this is a finding.

PDI:	DNS0735	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	DCCS-1, DCCS-2, ECSC-1, DCBP-1		
Vulnerability Description:	The named.conf options statement includes the phrase "rfc2308-type1 yes;”.		
Reference:	DNS STIG: Section 4.2.6.5		

8.4 IAVM Compliance

The following Information Assurance Vulnerability Management issuances affect DNS as an application and in some cases BIND specifically. In order to be fully compliant with IAVMs the systems must have a minimum BIND version of ISC BIND 9.3.1 or BIND 8.4.6.

- DNS8010 (2000-B-0001)
- DNS8020 (2000-B-0008)
- DNS8030 (2001-A-0001)
- DNS8040 (2002-A-0006)
- DNS8050 (2002-T-0010)
- DNS8060 (2003-B-0001)
- DNS8070 (2005-A-0005)

PDI:	DNS8010	Category:	I
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECND-1, ECND-2, ECSC-1		
Vulnerability Description:	IAVM notice, 2000-B-0001 has not been responded to.		
Reference:	DNS STIG: Appendix B		

PDI:	DNS8020	Category:	I
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECND-1, ECND-2, ECSC-1		
Vulnerability Description:	IAVM notice, 2000-B-0008 has not been responded to.		
Reference:	DNS STIG: Appendix B		

PDI:	DNS8030	Category:	I
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	

IA Controls:	ECND-1, ECND-2, ECSC-1
Vulnerability Description:	IAVM notice, 2001-A-0001 has not been responded to.
Reference:	DNS STIG: Appendix B

PDI:	DNS8040	Category:	I
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECND-1, ECND-2, ECSC-1		
Vulnerability Description:	IAVM notice 2002-A-0006 has not been responded to.		
Reference:	DNS STIG: Appendix B		

PDI:	DNS8050	Category:	I
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECND-1, ECND-2, ECSC-1		
Vulnerability Description:	IAVM notice, 2002-T-0010 has not been responded to.		
Reference:	DNS STIG: Appendix B		

PDI:	DNS8060	Category:	I
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECND-1, ECND-2, ECSC-1		
Vulnerability Description:	IAVM notice, 2003-B-0001 has not been responded to.		
Reference:	DNS STIG: Appendix B		

PDI:	DNS8070	Category:	I
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECND-1, ECND-2, ECSC-1		
Vulnerability Description:	IAVM notice, 2005-A-0005 has not been responded to. Vulnerable systems: ISC BIND 9.3.0 ISC BIND 8.4.4 ISC BIND 8.4.5		
Reference:	DNS STIG: Appendix B		

This page is intentionally left blank.

9. UNIX OS CONFIGURATION TO SUPPORT BIND

This section is to be used for each UNIX name server running BIND located at the site to be reviewed. This is in addition to the Name Server Security Requirements and the BIND Name Server Configuration section and is to be used for each and every UNIX OS name server running BIND. This section addresses security requirements related to BIND and the UNIX operating system in which BIND is running on.

The DNS SRR begins by completing the *Section 4.1*, *The Pre-Trip Preliminary Interview*, which includes obtaining answers to questions and gathering written documentation and procedures, and configuration and zone files prior to the onsite visit. In addition to the pre-trip information gathered, an SA will be required to assist in the console-based checks.

9.1 Vulnerabilities

Complete this entire form for each BIND instance running on a UNIX name server, which is being reviewed. For each PDI/VUL, check whether it is a finding or not a finding in the "Status" column. In cases in which the PDI/VUL is not applicable, check "Not Applicable" (e.g., it applies to an authoritative server, but you are reviewing a caching server). If a PDI/VUL is relevant to the environment, but you are unable to evaluate it for whatever reason (e.g., access restrictions or time limitations), then check "Not Reviewed."

9.1.1 Console-based Checks

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	Script	Status	Details		PDI/VUL	Description	Cat.
9.2.1		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS4440 V0003617	BIND is not configured to run as a dedicated non-privileged user account.	3
9.2.2		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS4450 V0003618	A UNIX or UNIX-based name server is running unnecessary daemon/services and/or is configured to start an unnecessary daemon, service, or program upon boot-up. (SNMP must be documented and configured in accordance with the UNIX STIG – this would not be a finding)	2

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	**Script**	**Status**	**Details**		**PDI/VUL**	**Description**	**Cat.**
9.2.3		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS4460 V0003619	It is possible to obtain a command shell by logging on to the DNS user account.	3
9.2.4		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS4470 V0003620	Permissions on critical UNIX name server files are not as restrictive as required.	2

9.2 Console-based Checks

This section of the review covers compliance with DNS STIG requirements that cannot be determined through the questionnaires, documentation, procedures, or configuration and zone files. Rather, validation of compliance with the requirements is determined via an operating system console. An authorized SA should perform the required actions. He or she will work side-by-side with the reviewer to determine which commands are most appropriate at certain points in the review.

For many of the UNIX checks, results of shell commands should be written to a newly created directory. Any directory will suffice. The instructions assume that the reviewer will use */etc/dns/srr*. If a floppy drive is available, writing to a floppy is preferable. The reviewer should work with the SA to set up the directory prior to beginning this segment of the review. The SA should also check available disk space. Although output in not expected to exceed a few kilobytes, this precautionary measure could avoid operational problems for servers with very little remaining disk space.

9.2.1 Dedicated User Account

Instruction: In the presence of the reviewer, the SA should enter the following command:

ps –ef | grep ‘named’ > /etc/dns/srr/bindUser.srr

The user identification (UID) utilized to run named should be found in the results. If the UID is root (i.e., 0) or another built-in ID, then this constitutes a finding. If it is not, then the next step is to check whether the UID is dedicated to this function. The SA should enter the following command, substituting the UID obtained in the previous step for *bindUID*:

ps –ef | grep ‘*bindUID*’ > bindUserDaemons.srr

If *bindUserDeamons.tmp* contains daemons/programs other than BIND (*named*), then this constitutes a finding. If the dedicated user is associated with *named* only, the next step is to check whether the user ID has any privileges other than those needed to run BIND. To accomplish this, the SA will check the following:

- Whether the BIND UID is a member of any group other than dnsgroup.
- Whether the BIND UID has permissions to any files other than key files and *named.stat.*

For the first item, the SA should run the following command (substituting the value for *bindUID* as appropriate):

grep ‘*bindUID*’ /etc/group > /etc/dns/srr/bindUserGroups.srr

For the second item, the SA should run the following command (substituting the name of the user ID for dnsuser if applicable):

find / -uid bindUID > /etc/dns/srr/bindUserFiles.srr

With regards to the first item, if *dnsuserGroups.srr* contains any entry other than dnsgroup (or its equivalent), then this constitutes a finding. With regards to the second item, if *dnsuserFilePermissions.srr* contains any entries other than the key files and *named.stat*, then this constitutes a finding.

PDI:	DNS4440	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECLP-1, ECCD-1, ECCD-2, ECPA-1, ECSC-1, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	BIND is not configured to run as a dedicated non-privileged user account.		
Reference:	DNS STIG: Appendix E.2		

9.2.2 Unnecessary Services

Instruction: The reviewer should examine the start-up files to determine whether they launch unnecessary programs. The file /etc/*inetd.conf* is common to UNIX implementations. The reviewer may use the **cat** command to view this file. If the file contains any of the following daemons, then this is a finding:

- admind
- chargen
- echo
- etherstatd
- fingerd
- ftpd
- httpd
- ICQ serve
- identd
- netstat
- netstatd
- nit
- nntp
- nsed
- nsemntd
- pfilt
- portd
- quaked
- rexd
- rexecd
- rje_mapper
- rlogind
- rpc_3270
- rpc_alias
- rpc_database
- rpc_keyserv
- rpc_sched
- rquotad
- rsh
- rstatd
- rusersd
- selectd
- serverd
- showfhd
- sprayd
- statmon
- sunlink_mapper
- sysstat
- talkd
- telnetd
- tfsd
- tftpd
- timed
- ttdb
- ugidd
- uucpd
- walld.

Below is a list of prohibited services. The name of the implementing Sun Solaris script and the file that launches it is found in parentheses. If any of these processes are running (the reviewer may use the **ps –ef | grep *service name*** to verify if the process is running or not), or configured to be started upon boot-up (the reviewer my use the **ls** command in the */etc/rc2.d* or */etc/rc3.d* directory), then this is a finding (although inherently dangerous, if SNMP is used for network management purposes, it must be documented and configured in accordance with the UNIX STIG):

- NFS client (s73nfs.client in rc2.d)
- automounter (s74autofs in rc2.d)
- printer queue daemon (s80lp in rc2.d)
- RPC portmapper (s71rpc in rc2.d)
- CDE login (s99dtlogin in rc2.d)
- NFS server process (s15nfs.server in rc3.d)
- SNMP daemon (s76snmpdx in rc3.d)

PDI:	DNS4450	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	DCPA-1, ECSC-1, DCBP-1		
Vulnerability Description:	A UNIX or UNIX-based name server is running unnecessary daemon/services and/or is configured to start an unnecessary daemon, service, or program upon boot-up. If SNMP is used for network management it must be documented and configured in accordance with the UNIX STIG.		
Reference:	DNS STIG: Appendix E.1		

9.2.3 Command Shell

Instruction: The SA should enter the following command (this command assumes that *named* is running as user dnsuser):

grep dnsuser /etc/passwd

Based on the command output, the reviewer can identify whether a shell exists for dnsuser. The shell should be */dev/null* or */bin/false*. If it is a legitimate shell, then this is a finding.

PDI:	DNS4460	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECLP-1, ECCD-1, ECCD-2, ECSC-1, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	It is possible to obtain a command shell by logging on to the DNS user account.		
Reference:	DNS STIG: Appendix E.2		

9.2.4 File Permissions

Instruction: Using the **ls –l** command from the directory containing the core BIND files, check that the permissions for the files listed are at least as restrictive as those listed in the table below:

FILE NAME	***OWNER***	***GROUP***	***PERMISSIONS***
named.conf	*root*	*dnsgroup*	*640*
named.pid	*root*	*dnsgroup*	*600*
named.run	*root*	*dnsgroup*	*660*
named_dump.db	*root*	*dnsgroup*	*660*
resolv.conf	*root*	*dnsgroup*	*640*
root hints file	*root*	*dnsgroup*	*640*
master zone file	*root*	*dnsgroup*	*640*
slave zone file	*root*	*dnsgroup*	*660*
TSIG key files	*dnsuser*	*dnsgroup*	*400*
named.stat	*dnsuser*	*dnsgroup*	*664*
log files other than the system logging facility	*dnsuser*	*dnsgroup*	*664*
ndc (FIFO)	*root*	*dnsgroup*	*600*
ndc.d (directory containing ndc)	*root*	*dnsgroup*	*700*

The *nmed.run* and *named_dump* files exist only on BIND 8 name servers. These files are generated using certain BIND control commands and may not be present. There is no finding if the files are not present, only if they are and do not have proper permissions. The *ndc* FIFO file and the *ndc.d* directory also are only found on BIND 8 name servers.

The name of the root hints file is defined in *named.conf*. Common names for the file are *root.hints, named.cache*, or *db.cache*.

Note that there may be multiple zone files, key files, and log files. The reviewer should be able to produce a list of the files based on a quick examination of *named.conf*, which is obtained in *Section 4.1.2, Pre-Trip Preliminary Documentation and Procedures*. The reviewer should check the permissions of each zone, key, or log file when more than one exists on the name server.

If permissions are more permissive than required, then this is a finding.

PDI:	DNS4470	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		ECLP-1, ECCD-1, ECCD-2, ECPA-1, ECSC-1, DCCS-1, DCCS-2, DCBP-1	
Vulnerability Description:		Permissions on critical UNIX name server files are not as restrictive as required.	
Reference:		DNS STIG: Appendix E.3.1	

10. WINDOWS OS CONFIGURATION TO SUPPORT BIND

This section is to be used for each Windows name server running BIND located at the site to be reviewed. This section is in addition to the Name Server Security Requirements and the BIND Name Server Configuration section and is to be used for each and every Windows OS name server running BIND. This addresses security requirements related to BIND and the Windows operating system, which BIND is running on.

The DNS SRR begins by completing the *Section 4.1, The Pre-Trip Preliminary Interview*, which includes obtaining answers to questions and gathering written documentation and procedures, and configuration and zone files prior to the onsite visit. In addition to the pre-trip information gathered, an SA will be required to assist in the console-based checks.

10.1 Vulnerabilities

Complete an entire form for each evaluated BIND instance running on a Windows name server, which is being reviewed. For each vulnerability, check whether it is a finding or not a finding in the “Status” column. In cases in which the vulnerability is not applicable, check “Not Applicable” (e.g., it applies to an authoritative server, but you are reviewing a resolving server). If a vulnerability is relevant to the environment, but you are unable to evaluate it for whatever reason (e.g., access restrictions or time limitations), then check “Not Reviewed.”

10.1.1 Console-based Checks

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	**Script**	**Status**	**Details**		**PDI/VUL**	**Description**	**Cat.**
10.2.1		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS4530 V0003621	ISC BIND is not configured to run as a dedicated non-privileged service user account.	2
10.2.2		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS4540 V0003622	The ISC BIND service user is a member of a group other than “Everyone” and “Authenticated Users”.	4
10.2.3		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS4550 V0003623	The ISC BIND service does not have the appropriate user rights required for the proper configuration and security of ISC BIND.	3
10.2.4		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS4570 V0003624	The appropriate encryption software is not correctly installed and configured on Windows ISC BIND name servers and it is required that in-band remote management be performed from hosts outside the enclave in which the name server resides.	2
10.2.5		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS4580 V0003625	Shares other than the default administrative shares are enabled on a name server.	2

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	**Script**	**Status**	**Details**		**PDI/VUL**	**Description**	**Cat.**
10.2.6		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS4590 V0003626	The ownership and permissions on all Windows ISC BIND name servers are not as restrictive as required.	2

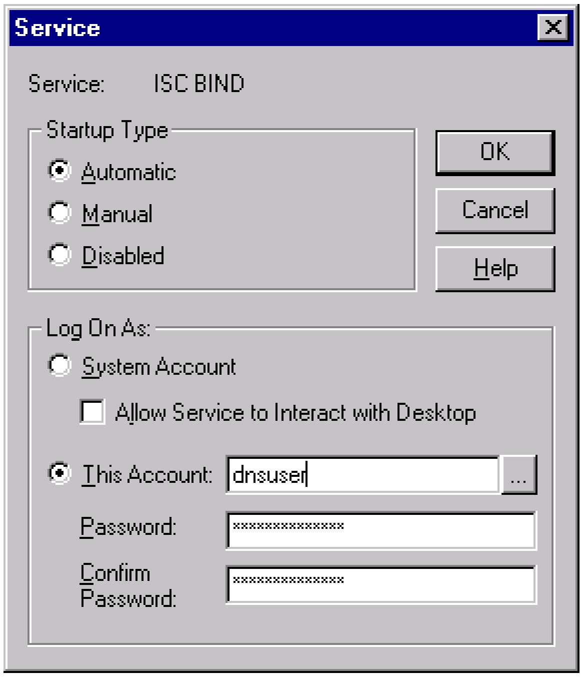
10.2 Console-based Checks

This section of the review covers compliance with DNS STIG requirements that cannot be determined through the questionnaires, documentation, procedures, or configuration and zone files. Rather, validation of compliance with the requirements is determined via an operating system console. An authorized SA should perform the required actions. He or she will work side-by-side with the reviewer to determine which commands are most appropriate at certain points in the review.

10.2.1 Dedicated User Account

- Windows NT

  Instruction: The reviewer will validate ISC BIND is configured to run as a dedicated non-privileged service user account. View the properties of the ISC BIND service (double-click on the ISC BIND service in the Windows Services GUI). In Windows NT 4.0 the following dialog box is displayed:



Service: ISC BIND

Startup Type

● Automatic
○ Manual
○ Disabled

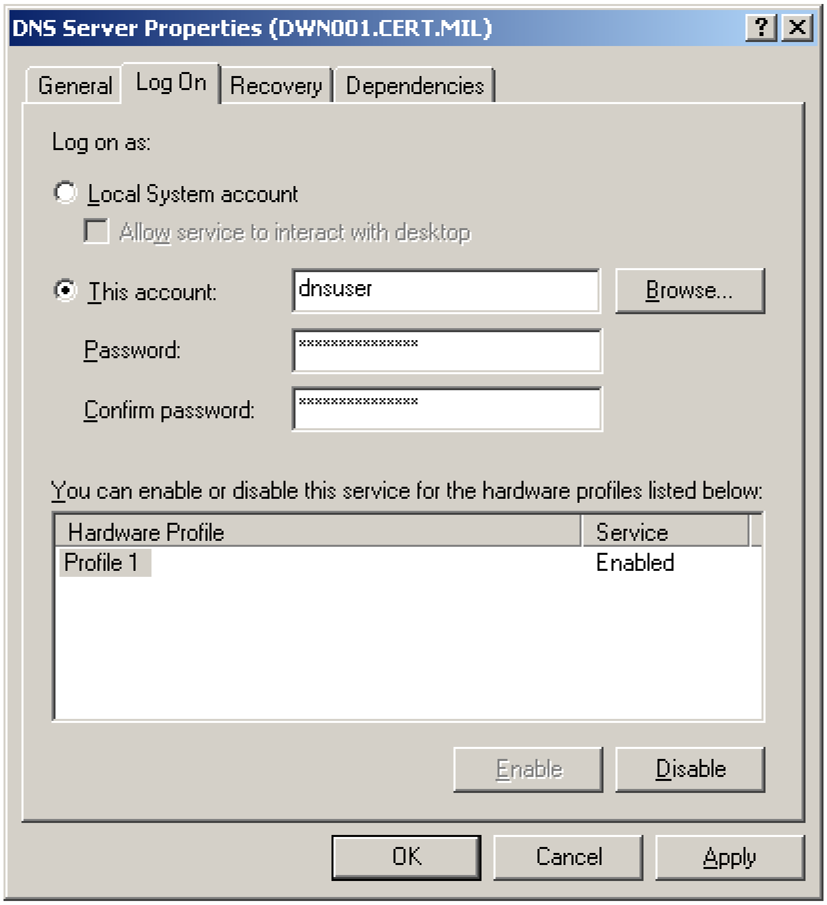
Log On As:

○ System Account
□ Allow Service to Interact with Desktop
● This Account: dnsuser
Password: ***************
Confirm Password: ***************

If the ISC BIND service logs on as the “System Account”, then this is a finding.

- Windows 2000

Instruction: The reviewer will validate ISC BIND is configured to run as a dedicated non-privileged service user account. Select the “Log On” tab of the properties of the ISC BIND service. In Windows 2000 the following dialog box is displayed:



DNS Server Properties (DWN001.CERT.MIL)

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: dnsuser

Password: xxxxxxxxxxxxxxx

Confirm password: xxxxxxxxxxxxxxx

You can enable or disable this service for the hardware profiles listed below:

Hardware Profile	Service
Profile 1	Enabled

If the ISC BIND service logs on as the “Local System account”, then this is a finding.

PDI:	DNS4530	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		ECLP-1, ECCD-1, ECCD-2, ECPA-1, ECSC-1, DCCS-1, DCCS-2, DCBP-1	
Vulnerability Description:		ISC BIND is not configured to run as a dedicated non-privileged service user account.	
Reference:		DNS STIG: Appendix F.2	

10.2.2 Group Membership

Instruction: In Windows NT, this can be accomplished by looking at the user's group properties in "User Manager." In Windows 2000, select System Tools | Users and Groups | Users in the "Computer Management" tool. View the "Member Of" tab in the "User Properties" dialog Box (which can be accessed by double-clicking on the user). If the user is a member of any group besides "everyone" and "Authenticated Users", then this is a finding.

In Windows, a user does not have to be a member of any group other than the implicit groups "Everyone" and "Authenticated Users." Thus, to best ensure security, dnsuser must be removed from all explicit groups, including the "Users" group, into which all users are placed by default. There should not be a dnsgroup group as is recommended for UNIX.

PDI:	DNS4540	Category:	IV
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		ECLP-1, ECCD-1, ECCD-2, ECPA-1, ECSC-1, DCCS-1, DCCS-2, DCBP-1	
Vulnerability Description:		The ISC BIND service user is a member of a group other than "Everyone" and "Authenticated Users."	
Reference:		DNS STIG: Appendix F.2	

10.2.3 Service User Rights

Instruction: In Windows NT, select User Rights from the menu bar in "User Manager." Select each user right and confirm that the DNS user account is not listed under any rights assignment other than "log on as a service." If it is, this is a finding.

Windows 2000 is similar to Windows NT, but adds several relevant user rights (actually user prohibitions). In "Local Security Settings" (a Microsoft Management Console Plug-in), select Local Policies | User Rights Assignments in the left windowpane. By looking at the assignments in the right windowpane, check that the DNS user account is not listed under any assignments other than "Log on as a service," "Deny access to this computer from the network," and "Deny logon as batch job." If the user has any additional rights beyond these, this is a finding.

PDI:	DNS4550	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		ECLP-1, ECCD-1, ECCD-2, ECPA-1, ECSC-1, DCCS-1, DCCS-2, DCBP-1	
Vulnerability Description:		The ISC BIND service does not have the appropriate user rights required for the proper configuration and security of ISC BIND.	
Reference:		DNS STIG: Appendix F.2	

10.2.4 Encryption Software and Remote Management

FOLDER/FILE NAME	***OWNER***	***USER/GROUP***	***PERMISSIONS***
%systemroot%\system32\dns\bin	*administrators*	*administrators*	*Full control*
		dnsadmins	*Read*
		dnsuser	*Read*
%systemroot%\system32\dns\etc	*administrators*	*administrators*	*Full control*
		dnsadmins	*Change*
		dnsuser	*Change*
named.conf	*administrators*	*administrators*	*Full control*
		dnsadmins	*Change*
		dnsuser	*Read*
named.pid	*administrators*	*administrators*	*Full control*
		dnsadmins	*Read*
		dnsuser	*Change*
named.cache	*administrators*	*administrators*	*Full control*
		dnsadmins	*Change*
		dnsuser	*Read*
any zone file	*administrators*	*administrators*	*Full control*
		dnsadmins	*Change*
		dnsuser	*Change*
any TSIG key file	*administrators*	*dnsuser*	*Read*
root hints file	*administrators*	*administrators*	*Full control*
		dnsadmins	*Read*
		dnsuser	*Change*
log files other than the Event Viewer files.	*administrators*	*administrators*	*Full control*
		dnsadmins	*Read*
		dnsuser	*Change*

Instruction: During Question H in *Section 4.2.1, Network Specialist Interview Questions*, the Network Specialist interview (or other conversation), a DNS or Systems Administrator may state that the evaluated Windows BIND name server is administered from a host outside of the internal network (e.g., a home office or remote site). In this case, there must be appropriate software on the Windows BIND name server to support encrypted communication. Once the service has been identified, the reviewer should check that the software does require encrypted sessions and authentication. Additional checks from the Secure Remote Computing STIG may apply. If the reviewer determines that the installed remote access/control configuration is inadequate, then there should be a finding with a written explanation specifying why the configuration is inadequate.

PDI:	DNS4570	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		DCNR-1, ECSC-1, DCCS-1, DCCS-2, DCBP-1	
Vulnerability Description:		The appropriate encryption software is not correctly installed and configured on Windows ISC BIND name servers and it is required that in-band remote management be performed from hosts outside the enclave in which the name server resides.	
Reference:		DNS STIG: Appendix F.1	

10.2.5 Shares

Instruction: From a command prompt, type **net view \\127.0.0.1** and press enter. If any shares appear other than default administrative shares (e.g., C$, NETLOGON$), then this is a finding.

PDI:	DNS4580	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		ECLP-1, ECCD-1, ECCD-2, ECPA-1, ECSC-1, DCCS-1, DCCS-2, DCBP-1	
Vulnerability Description:		Shares other than the default administrative shares are enabled on a name server.	
Reference:		DNS STIG: Appendix F.1	

10.2.6 File Permissions

Instruction: The reviewer can check permissions and ownership by looking at the properties of each file in “Windows Explorer.”

Note that there may be multiple zone files, key files, and log files. The reviewer should be able to produce a list of the files based on a quick examination of *named.conf*, which should have been obtained at the beginning of this module. The reviewer should check the permissions of each zone, key or log file when more than one exists on the name server.

The name of the root hints file is defined in named.conf. Common names for the root hints file are *root.hints*, *named.cache,* and *db.cache*.

If permissions are more permissive than required, then this is a finding.

PDI:	DNS4590	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		ECLP-1, ECCD-1, ECCD-2, ECPA-1, ECSC-1, DCCS-1, DCCS-2, DCBP-1	
Vulnerability Description:		The ownership and permissions on all Windows ISC BIND name servers are not as restrictive as required.	
Reference:		DNS STIG: Appendix F.3	

This page is intentionally left blank.

11. WINDOWS 2000 DNS NAME SERVER

This section is to be used for each Windows 2000 DNS implementation located at the site to be reviewed. This section is in addition to the Name Server Security Requirements and is to be used for each and every Windows 2000 DNS name server. This section addresses security requirements related to Windows 2000 DNS.

The DNS SRR begins by completing the *Section 4.1, The Pre-Trip Preliminary Interview*, which includes obtaining answers to questions and gathering written documentation and procedures, and configuration and zone files prior to the onsite visit. In addition to the pre-trip information gathered, completion of *Section 4.2, The Network Specialist Interview,* is required to accurately complete this section.

11.1 Vulnerabilities

Complete an entire form for each evaluated Windows 2000 DNS name server. For each vulnerability check whether it is a finding or not a finding in the “Status” column. In cases in which the vulnerability is not applicable, check “Not Applicable” (e.g., it applies to an authoritative server, but you are reviewing a resolving server). If a vulnerability is relevant to the environment, but you are unable to evaluate it for whatever reason (e.g., access restrictions or time limitations), then check “Not Reviewed.”

11.1.1 Checks Associated with Interview Responses

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	**Script**	**Status**	**Details**		**PDI/VUL**	**Description**	**Cat.**
11.2.1		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0800 V0004500	The firewall rules or router ACLs do not prevent unauthorized hosts from outside the enclave from querying Windows 2000 DNS servers.	2

11.1.2 Console-based Checks

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	Script	Status	Details		PDI	Description	Cat.
11.3.1		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0805 V0004501	The DHCP server service is not disabled on any Windows 2000 DNS server that supports dynamic updates.	1
11.3.2		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0810 V0004502	Zone transfers are not prohibited or a VPN solution is not implemented that requires cryptographic authentication of communicating devices and is used exclusively by name servers authoritative for the zone.	1
11.3.3		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0815 V0004503	Forwarders on an authoritative Windows 2000 DNS server are not disabled.	2
11.3.4		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0820 V0004504	Recursion on an authoritative Windows 2000 DNS server is not disabled.	2
11.3.5		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0825 V0004505	WINS lookups is not prohibited on a Windows 2000 DNS server.	1

11.2 Checks Associated with Interview Responses

The questions asked during *Section 4.2.1, Network Specialist Interview Questions,* will enable the reviewer to complete this section.

11.2.1 Queries

Instruction: If the answer to Question E and F in *Section 4.2.1*, *Network Specialist Interview Questions*, demonstrates that there is access to a Windows 2000 DNS server from outside of the enclave, then this is a finding.

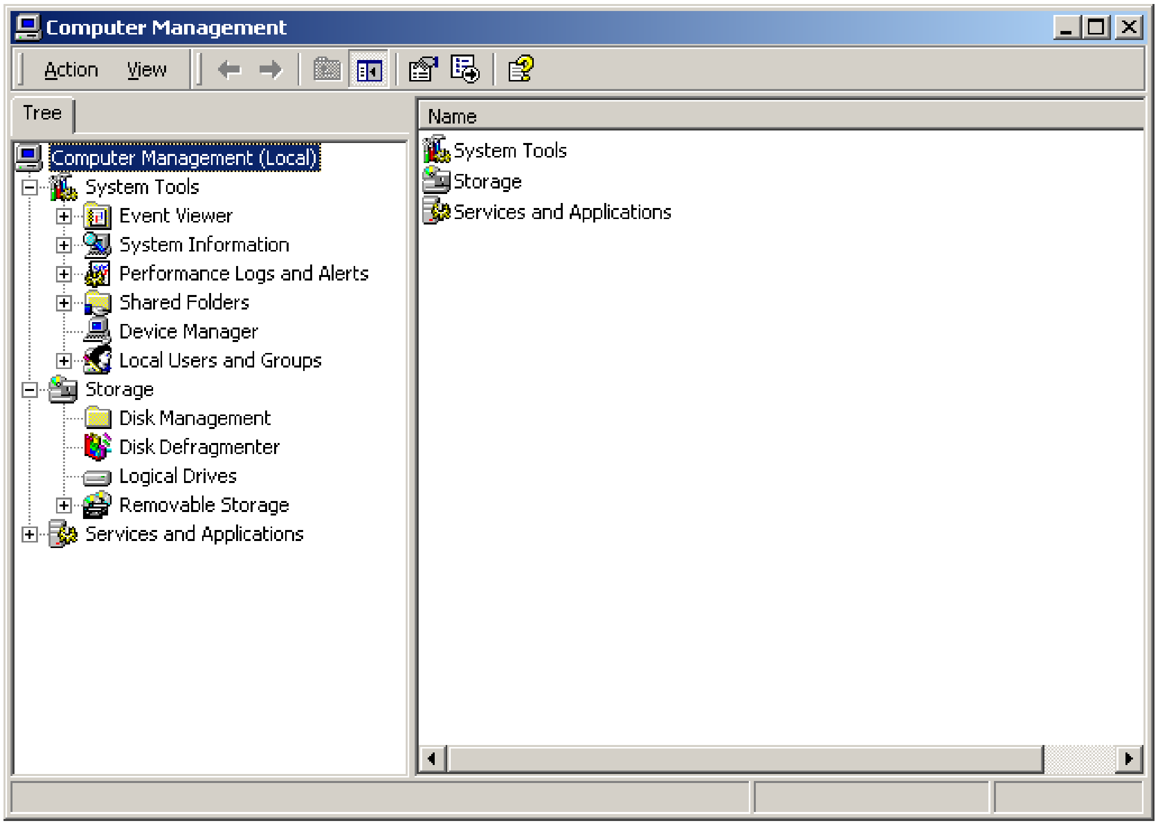
PDI:	DNS0800	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	IAIA-1, ECSC-1, ECCD-1, ECCD-2, DCBP-1		
Vulnerability Description:	The firewall rules or router ACLs do not prevent unauthorized hosts from outside the enclave from querying Windows 2000 DNS servers.		
Reference:	DNS STIG: Sec. 5.2		

11.3 Console-based Checks

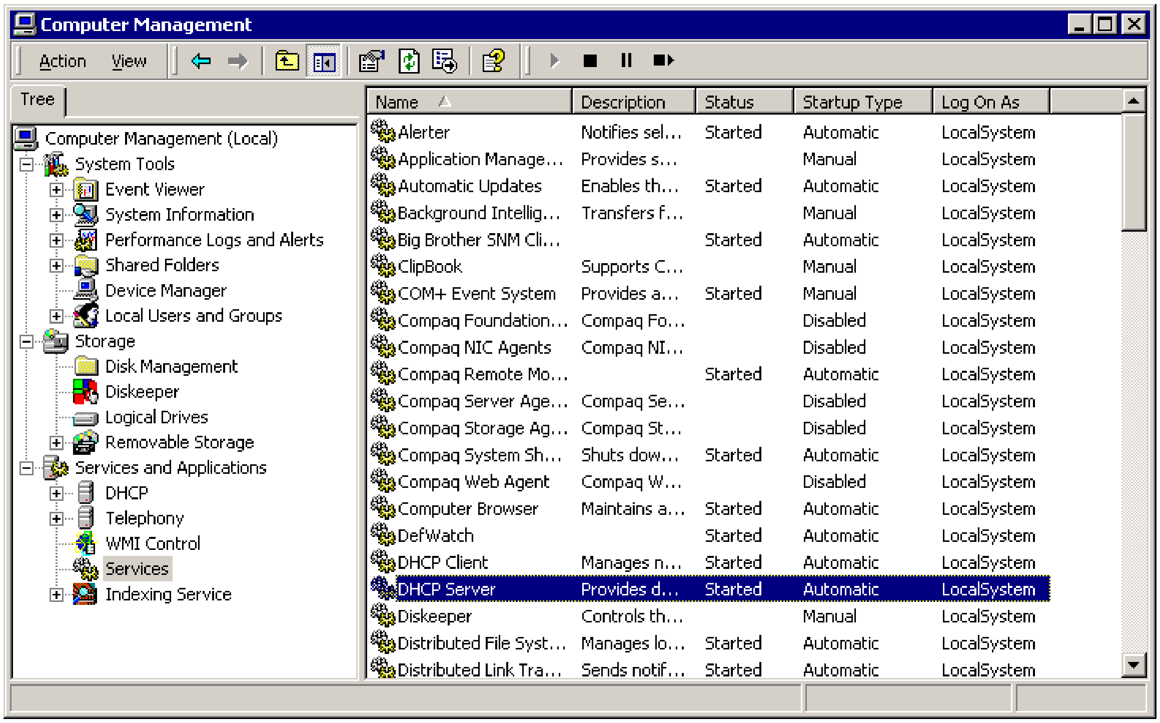
This section of the review covers compliance with DNS STIG requirements that cannot be determined through the questionnaires, documentation, procedures, or configuration and zone files. Rather, validation of compliance with the requirements is determined via an operating system console. An authorized SA should perform the required actions. He or she will work side-by-side with the reviewer to determine which commands are most appropriate at certain points in the review.

11.3.1 DHCP Server Service

Instruction: Log in to the server with an account that has admin rights. Right-click “My Computer” on the desktop and click “Manage.” This brings up the “Computer Management” tool as pictured below.

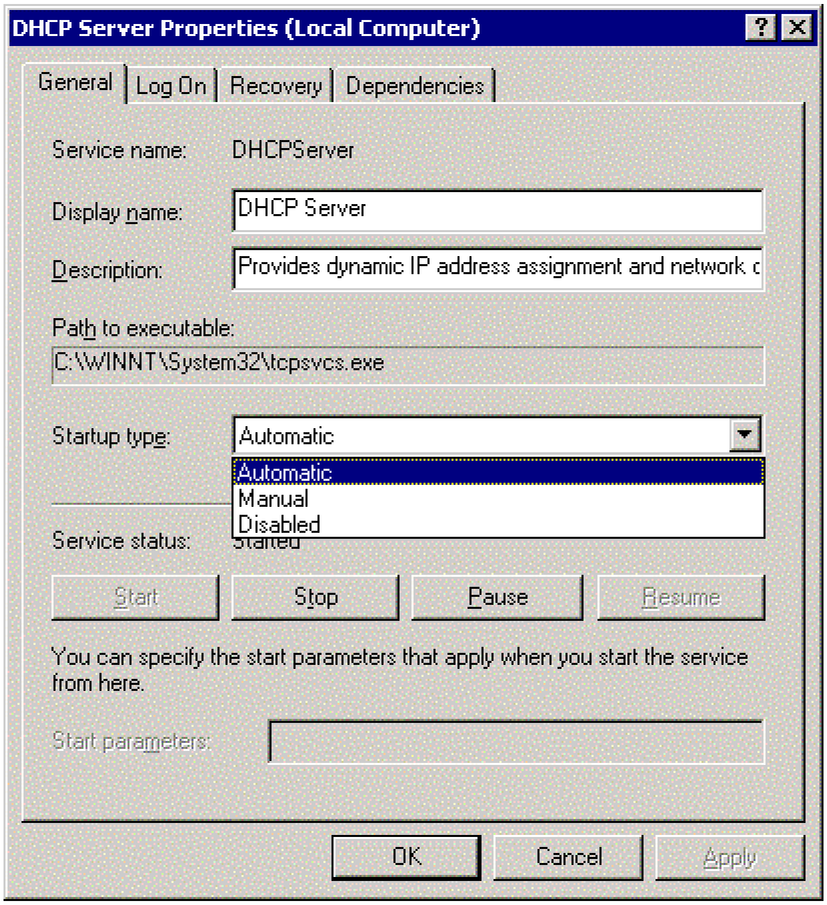


Instruction: Click the plus sign next to “Services and Applications” on the left pane to expand it. Select “Services” on the left pane, as pictured below.



Name	Description	Status	Startup Type	Log On As
Alerter	Notifies sel...	Started	Automatic	LocalSystem
Application Manage...	Provides s...		Manual	LocalSystem
Automatic Updates	Enables th...	Started	Automatic	LocalSystem
Background Intellig...	Transfers f...		Manual	LocalSystem
Big Brother SNM Cli...		Started	Automatic	LocalSystem
ClipBook	Supports C...		Manual	LocalSystem
COM+ Event System	Provides a...	Started	Manual	LocalSystem
Compaq Foundation...	Compaq Fo...		Disabled	LocalSystem
Compaq NIC Agents	Compaq NI...		Disabled	LocalSystem
Compaq Remote Mo...		Started	Automatic	LocalSystem
Compaq Server Age...	Compaq Se...		Disabled	LocalSystem
Compaq Storage Ag...	Compaq St...		Disabled	LocalSystem
Compaq System Sh...	Shuts dow...	Started	Automatic	LocalSystem
Compaq Web Agent	Compaq W...		Disabled	LocalSystem
Computer Browser	Maintains a...	Started	Automatic	LocalSystem
DefWatch		Started	Automatic	LocalSystem
DHCP Client	Manages n...	Started	Automatic	LocalSystem
DHCP Server	Provides d...	Started	Automatic	LocalSystem
Diskeeper	Controls th...		Manual	LocalSystem
Distributed File Syst...	Manages lo...	Started	Automatic	LocalSystem
Distributed Link Tra...	Sends notif...	Started	Automatic	LocalSystem

Instruction: On the right pane, scroll down and select "DHCP Server." Right-click "DHCP Server" and click "Properties." This brings up the "DCHP Server Properties" page as pictured below.



DHCP Server Properties (Local Computer)

Service name: DHCPServer

Display name: DHCP Server

Description: Provides dynamic IP address assignment and network c

Path to executable:
C:\WINNT\System32\tcpsvcs.exe

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

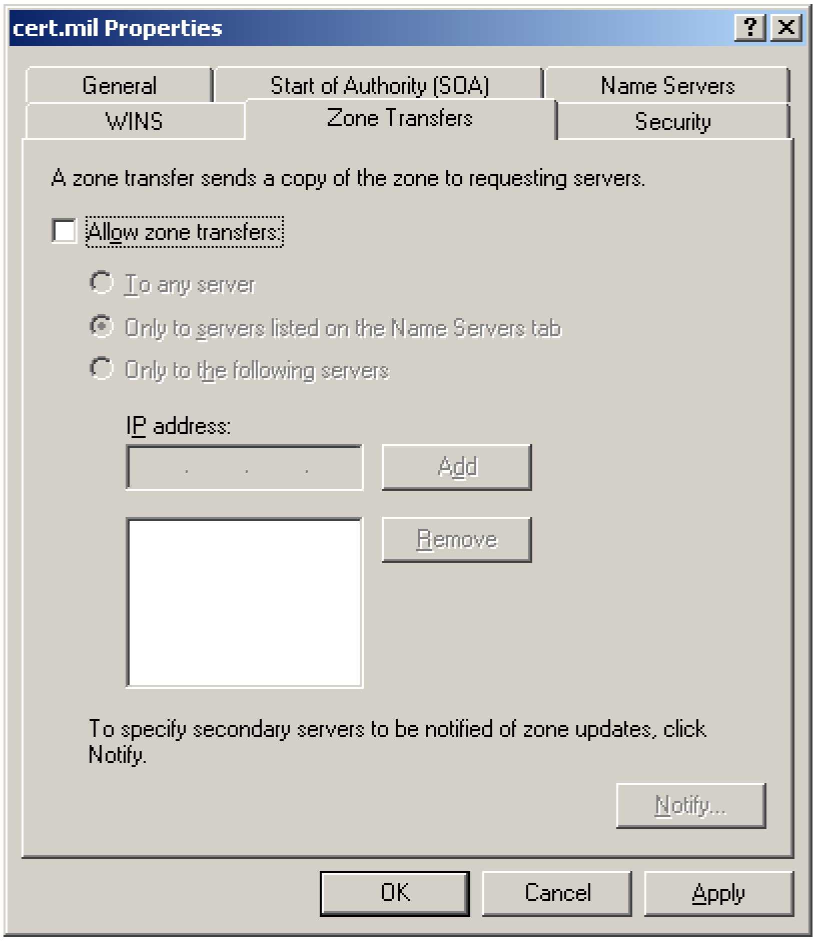
Start parameters:

Instruction: The reviewer will validate the DHCP server service is disabled. The "Disabled" drop down selection is to be selected on the "General" tab of the "DHCP Server Properties." If the DHCP server service is not disabled, then this is a finding.

PDI:	DNS0805	Category:	I
MAC/Confidentiality Levels:	MAC I – CSP, MAC II – CSP, MAC III – CSP		
IA Controls:	ECLP-1, ECCD-1, ECCD-2, ECSC-1, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	The DHCP server service is not disabled on any Windows 2000 DNS server that supports dynamic updates.		
Reference:	DNS STIG: Sec. 5.3		

11.3.2 Zone Transfers

Instruction: The reviewer will validate zone transfers are prohibited. The reviewer will ensure the "Allow zone transfers" check box is not selected on the “Zone Transfers” tab of the name server properties.



A zone transfer sends a copy of the zone to requesting servers.

□ Allow zone transfers:

○ To any server

● Only to servers listed on the Name Servers tab

○ Only to the following servers

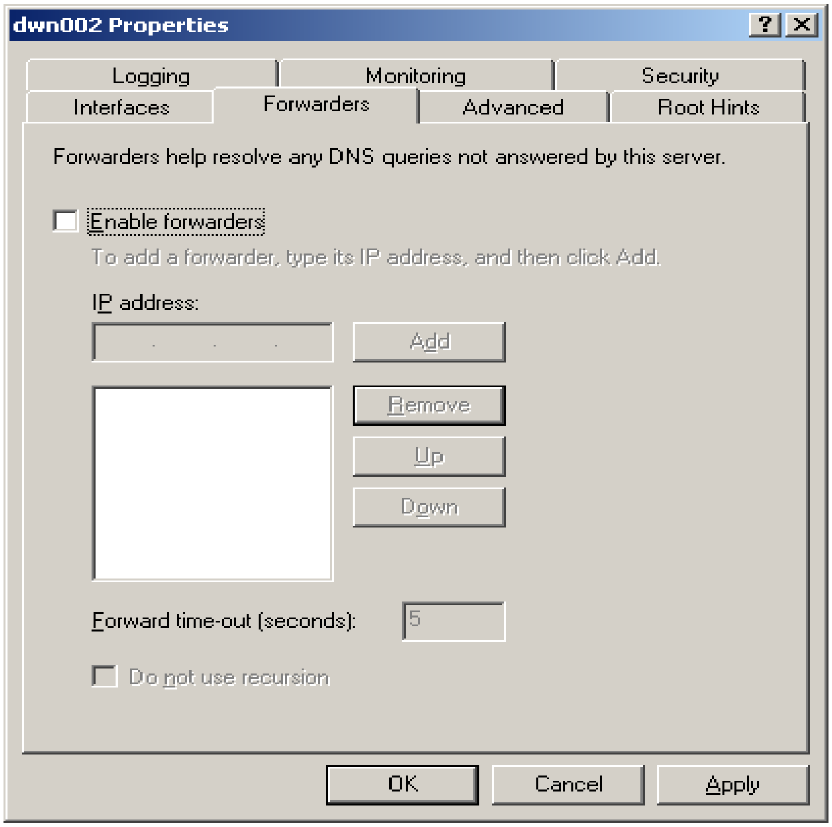
To specify secondary servers to be notified of zone updates, click Notify.

If zone transfers are allowed, then this is a finding.

PDI:	DNS0810	Category:	I
MAC/Confidentiality Levels:	MAC I – CSP, MAC II – CSP, MAC III – CSP		
IA Controls:	ECLP-1, ECCD-1, ECCD-2, ECSC-1, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	Zone transfers are not prohibited or a VPN solution is not implemented that requires cryptographic authentication of communicating devices and is used exclusively by name servers authoritative for the zone.		
Reference:	DNS STIG: Sec. 5.4		

11.3.3 Forwarders

Instruction: Windows 2000 DNS should not be deployed as a caching name server. Consequently, the use of forwarders and recursion is prohibited on Windows 2000 DNS. The reviewer will validate that the "Enable Forwarders" check box is not selected on the “Forwarders” tab of the name server properties, as pictured below:



Forwarders help resolve any DNS queries not answered by this server.

□ Enable forwarders

To add a forwarder, type its IP address, and then click Add.

IP address:

Forward time-out (seconds): 5

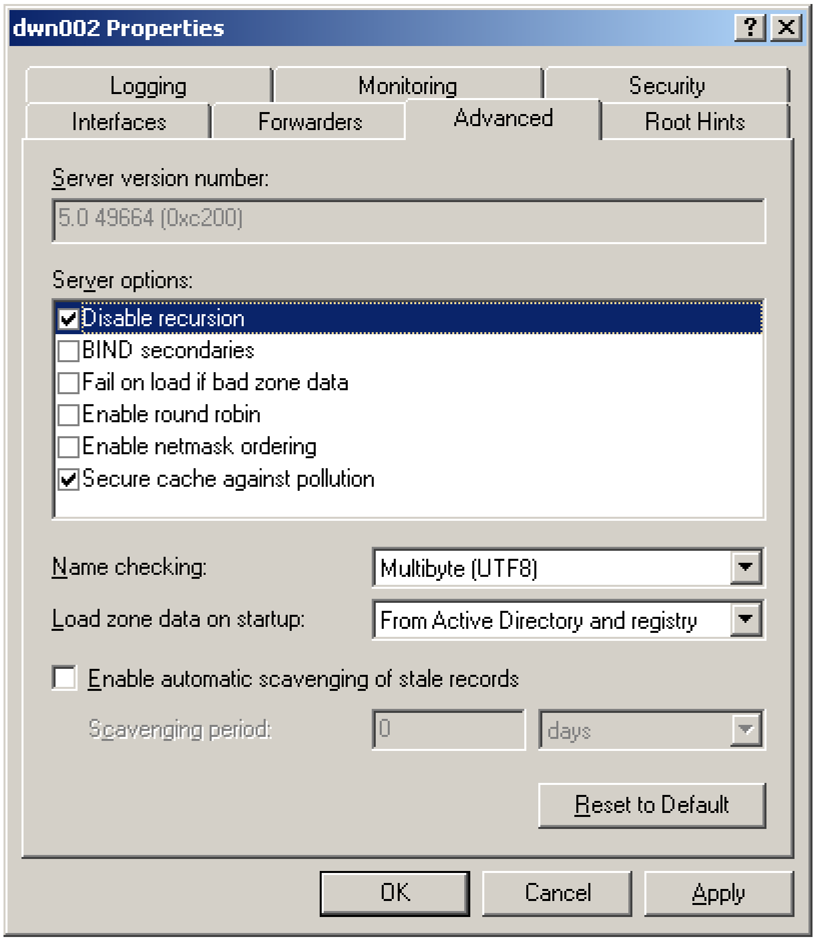
□ Do not use recursion

If forwarders are enabled, then this is a finding.

PDI:	DNS0815	Category:	II
MAC/Confidentiality Levels:	MAC I – CSP, MAC II – CSP, MAC III – CSP		
IA Controls:	ECSC-1, ECCD-1, ECCD-2, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	Forwarders on an authoritative Windows 2000 DNS server are not disabled.		
Reference:	DNS STIG: Sec. 5.5		

11.3.4 Recursion

Instruction: Windows 2000 DNS should not be deployed as a caching name server. Consequently, the use of forwarders and recursion is prohibited on Windows 2000 DNS. The reviewer will validate that the "Disable recursion" and the “Secure cache against pollution" on the “Advanced” tab of the name server properties are selected, as pictured below:



Server version number: 5.0 49664 (0xc200)

Server options:
☑ Disable recursion
□ BIND secondaries
□ Fail on load if bad zone data
□ Enable round robin
□ Enable netmask ordering
☑ Secure cache against pollution

Name checking: Multibyte (UTF8)

Load zone data on startup: From Active Directory and registry

□ Enable automatic scavenging of stale records

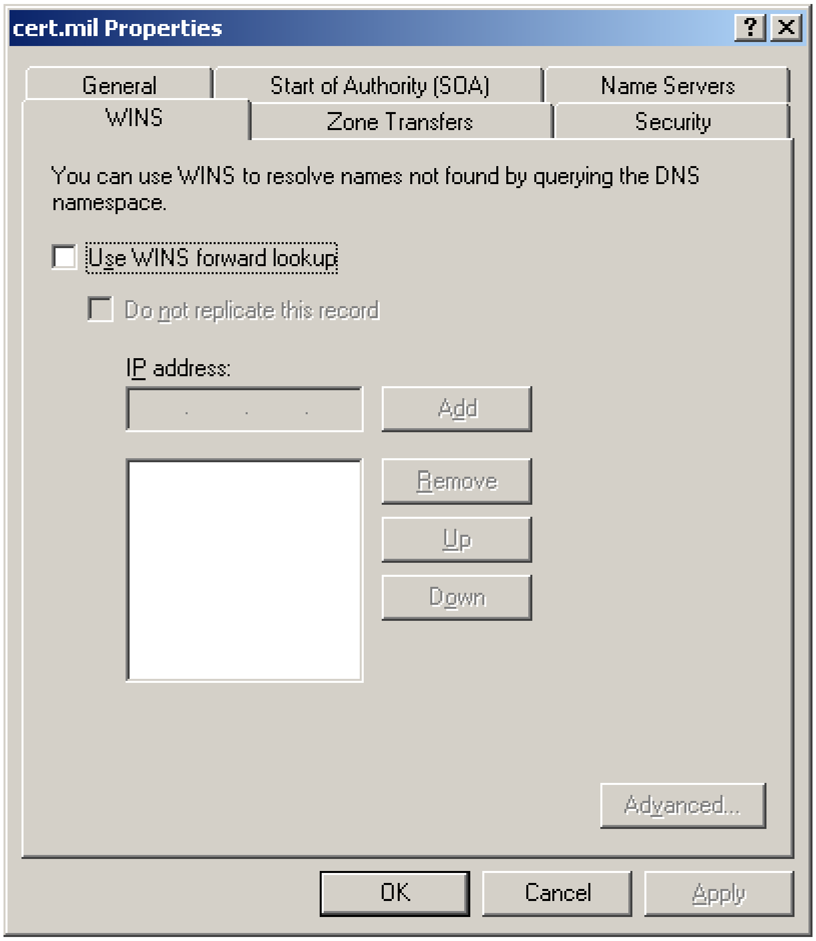
Scavenging period: 0 days

If recursion is not disabled, then this is a finding.

PDI:	DNS0820	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECSC-1, ECCD-1, ECCD-2, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	Recursion on an authoritative Windows 2000 DNS server is not disabled.		
Reference:	DNS STIG: Sec. 5.5		

11.3.5 WINS Integration

Instruction: The reviewer will validate the "Use WINS forward lookup" is not checked on the “WINS” tab on the properties dialog of each zone, as pictured below.



cert.mil Properties

You can use WINS to resolve names not found by querying the DNS namespace.

□ Use WINS forward lookup

□ Do not replicate this record

IP address:

If WINS is integrated on a Windows 2000 DNS server, then this is a finding.

PDI:	DNS0825	Category:	I
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	ECSC-1, ECCD-1, ECCD-2, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	WINS lookups is not prohibited on a Windows 2000 DNS server.		
Reference:	DNS STIG: Sec. 5.6		

This page is intentionally left blank.

12. CISCO CSS CONFIGURATION

This section is to be used for each Cisco CSS DNS device that is being reviewed. This section is in addition to the Name Server Security Requirements and is to be used for each and every Cisco CSS device. This section addresses security requirements related to Cisco CSS DNS.

The DNS SRR begins by completing the *Section 4.1, The Pre-Trip Preliminary Interview*, which includes obtaining answers to questions and gathering written documentation and procedures, and configuration and zone files prior to the onsite visit. In addition to the pre-trip information gathered, completion of *Section 4.5, The CSS Interview*, is required to accurately complete this section. Additionally, a CSS DNS administrator will be required to assist in the console-based checks.

This page is intentionally left blank.

12.1 Vulnerabilities

Complete this entire form for each CSS DNS instance being reviewed. For each PDI/VUL, check whether it is a finding or not a finding in the “Status” column. In cases in which the PDI/VUL is not applicable, check “Not Applicable” (e.g., it applies to an authoritative server, but you are reviewing a caching server). If a PDI/VUL is relevant to the environment, but you are unable to evaluate it for whatever reason (e.g., access restrictions or time limitations), then check “Not Reviewed.”

12.1.1 Checks Associated with Interview Responses

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	**Script**	**Status**	**Details**		**PDI/VUL**	**Description**	**Cat.**
12.2.1		☐ Finding ☐ Not a Finding ☐ Not Applicable ☐ Not Reviewed			DNS0900 V0004506	The shared secret in the APP session(s) was not a randomly generated 32-character text string.	3

12.1.2 Console-based Checks

Procedure Section Headings		Finding Information			PDI/VUL Information		
Manual	**Script**	**Status**	**Details**		**PDI/VUL**	**Description**	**Cat.**
12.3.1		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0905 V0004507	The Cisco CSS DNS is utilized to host the organization’s authoritative records and DISA Computing Services does not support that host in its csd.disa.mil domain and associated high-availability server infrastructure.	2
12.3.2		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0910 V0004508	Zones are delegated with the CSS DNS.	3
12.3.3		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0915 V0004512	CSS DNS does not cryptographically authenticate APP sessions.	3
12.3.4		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0920 V0004509	The CSS DNS does not transmit APP session data over an out-of-band network if one is available.	3
12.3.5		□ Finding □ Not a Finding □ Not Applicable □ Not Reviewed			DNS0925 V0004510	Forwarders are not disabled on the CSS DNS.	3

12.2 Checks Associated with Interview Responses

The questions asked in *Section 4.4.1 CSS Administrator Interview Questions*, will enable the reviewer to complete this section.

12.2.1 Session Key

Instruction: Using the answer to Question A in *Section 4.5.1, CSS Administer Interview Questions*, if the key was not a randomly generated 32-character text string then this is a finding.

PDI:	DNS0900	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		DCCS-1, DCCS-2, ECSC-1, DCBP-1	
Vulnerability Description:		The shared secret in the APP session(s) was not a randomly generated 32-character text string.	
Reference:		DNS STIG: Section 6.3	

12.3 Console-based Checks

This section of the review covers compliance with DNS STIG requirements that cannot be determined through the questionnaires, documentation, procedures, or configuration and zone files. Rather, validation of compliance with the requirements is determined via an operating system console. The CSS DNS administrator should perform the required actions. He or she will work side-by-side with the reviewer to determine which commands are most appropriate at certain points in the review.

12.3.1 Authoritative Records

Instruction: Using the answer to Question C in *Section 4.1.1, Pre-Trip Preliminary Interview Questions,* determine whether the CSS DNS device is used as an authoritative name server. If the CSS DNS does maintain authoritative records, then this is a finding. The exception to this is if this CSS DNS device supports authoritative records for a host(s) within the csd.disa.mil domain, which is not a finding.

Instruction: In the presence of the reviewer, the CSS DNS administrator should enter the following command while in global configuration mode:

```
show dns-record statistics
```

If any of the hosts have domain names outside of the csd.disa.mil domain, then this is a finding.

PDI:	DNS0905	Category:	II
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		DCCS-1, DCCS-2, ECSC-1, DCBP-1	
Vulnerability Description:		The Cisco CSS DNS is utilized to host the organization's authoritative records and DISA Computing Services does not support that host in its csd.disa.mil domain and associated high-	

	availability server infrastructure.
Reference:	DNS STIG: Section 6.2.1

12.3.2 Zone Delegation

Instruction: In the presence of the reviewer, the CSS DNS administrator should enter the following command while in global configuration mode:

show dns-record statistics

There should be no DNS record types of NS. If there are NS records, then this is a finding.

PDI:	DNS0910	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	DCCS-1, DCCS-2, ECSC-1, DCBP-1		
Vulnerability Description:	Zones are delegated with the CSS DNS.		
Reference:	DNS STIG: Section 6.2.2		

12.3.3 Session Authentication and Encryption

Instruction: In the presence of the reviewer, the CSS DNS administrator should enter the following command while in global configuration mode:

show app session

Confirm the authentication type is set to “authChallenge” and the encryption type is set to “encryptMd5hash.” This will confirm APP CHAP authentication and MD5 hashing features for APP sessions are configured between peers, if this is not the case, then this is a finding. The only exception would be if the CSS DNS administrator uses an IPSEC VPN between each peer couple. Review the IPSEC VPN with the CSS DNS administrator and validate the IPSEC VPN is configured between peers, if this is not the case, then this is a finding.

PDI:	DNS0915	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:	IAIA-1, DCNR-1, ECSC-1, ECCD-1, ECCD-2, DCCS-1, DCCS-2, DCBP-1		
Vulnerability Description:	CSS DNS does not cryptographically authenticate APP sessions.		
Reference:	DNS STIG: Section 6.3		

12.3.4 APP Session Data

Instruction: In the presence of the reviewer, the CSS DNS administrator should enter the following command while in global configuration mode:

```
show app session
```

Instruction: Compare the output of the above mentioned command and the answer to Question A in *Section 4.2.1, Network Specialist Interview Questions*, ensure Application Peering Protocol (APP) session data is not sent over an out-of-band network. If APP session data is sent over an out-of-band network, then this is a finding.

PDI:	DNS0920	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		ECSC-1, DCCS-1, DCCS-2, DCBP-1	
Vulnerability Description:		The CSS DNS does not transmit APP session data over an out-of-band network if one is available.	
Reference:		DNS STIG: Section 6.3	

12.3.5 Forwarders

Instruction: In the presence of the reviewer, the CSS DNS administrator should enter the following command while in global configuration mode:

```
show dns-server forwarder
```

Confirm the DNS server forwarder primary and DNS server forwarder secondary are "Not Configured." If either of these is configured, then this is a finding.

PDI:	DNS0925	Category:	III
MAC/Confidentiality Levels:		MAC I – CSP, MAC II – CSP, MAC III – CSP	
IA Controls:		ECSC-1, ECCD-1, ECCD-2, DCCS-1, DCCS-2, DCBP-1	
Vulnerability Description:		Forwarders are not disabled on the CSS DNS.	
Reference:		DNS STIG: Section 6.5	

This page is intentionally left blank.

APPENDIX A. SURVEY INSTRUMENTS

This Appendix contains several survey instruments that can assist reviewers with the conduct of a DNS SRR. The interview questions are also listed in the main body of the document. They are repeated here in a format that more conducive to copying. A reviewer may choose to make a copy of these pages before conducting the interviews.

A.1 The Pre-Trip Preliminary Interview Survey Instrument

Many of the answers to these questions will also be entered into the introductory sections of the SRR Report. The reviewer may choose to put the answer directly into those tables or first write them down here.

A. What DNS domains are associated with the organization for which the site has responsibility?

B. How are the domains aggregated into DNS zones?

C. For each zone, what are the host names and physical locations of each of the name servers supporting that zone? Which of these is the master name server for the domain, and which are slaves?

D. What are the host names and physical locations of each of the name servers that resolve DNS queries on behalf of DNS client computers over which the site has responsibility? (These could possibly be the same name servers specified in the answer to Question C.)

E. Who is an appropriate person who can provide DNS SRR personnel with information related to the network infrastructure, including IP network, router and firewall configuration. This might be the Network Security Officer, DNS Administrator, or another individual with a good working knowledge of the local environment. What is the phone number and e-mail address of this individual?

F. Who is an appropriate person to provide DNS SRR personnel with a facility tour in which the personnel can see the name servers, supporting network infrastructure, and associated physical and environmental controls. What is the phone number and e-mail address of this individual?

G. For each name server undergoing evaluation, what software currently provides DNS server functionality (e.g., BIND, CSS, and/or Windows 2000 DNS)? What version of the software is installed (e.g., BIND 9.2.1)?

A.2 The Network Specialist Interview Survey Instrument

Many of the answers to these questions will also be entered into the introductory sections of the SRR Report. The reviewer may choose to put the answer directly into those tables or first write them down here.

A. What IP networks and subnets comprise the internal network?

B. What IP subnets comprise the organization's DMZ(s)?

C. What is the physical location (building or site) of each of the networks or subnets specified in the responses to Question A and B?

D. What is the IP address and subnet mask of each of the name servers listed in response to Pre-Trip Preliminary Interview Question C?

E. Where are firewall devices located within the network infrastructure? What are the IP addresses of each of the firewall interfaces?

F. How do firewall rules and router ACLs restrict access to the listed name servers? Which of the name servers are accessible from external hosts?

G. If Network Address Translation (NAT) is used for particular hosts in a DMZ or on an internal network, then what the actual and translated IP addresses for those hosts?

H. Does anyone in the organization administer a name server from a computer residing outside of the enclave? If yes, where are the clients located and which name servers are administered in this manner? What software, if any, is used to encrypt network traffic between client and server?

A.3 The DNS Administrator Interview Survey Instrument

A. How are DNS logs archived (i.e., to what storage medium using what process?) How long are the archived files stored before deletion or destruction?

B. How are operating system logs archived (i.e., to what storage medium using what processes)? How long are the archived files stored before deletion or destruction?

A.4 The CSS Interview Survey Instrument

A. What is the length of the session_key used when configuring the APP CHAP authentication and MD5? How was the key generated (i.e., randomly created)?

This page is intentionally left blank.

This page is intentionally left blank.